Annex B – Australia's participation in the CBPR

APEC CROSS-BORDER PRIVACY RULES SYSTEM PROGRAM REQUIREMENTS: ENFORCEMENT MAP

As outlined in the Charter of the APEC Cross Border Privacy Rules (CBPR) System's Joint Oversight Panel (JOP), an APEC Member Economy is considered a Participant in the CBPR System after the Chair of the Electronic Commerce Steering Group (ECSG Chair) has notified the Economy that the following conditions have been met:

(i) The Economy's ECSG delegation, or appropriate governmental representative, submits to the ECSG Chair a letter indicating its intention to participate and confirming that at least one Privacy Enforcement Authority in that Economy is a participant in the APEC Cross Border Privacy Enforcement Arrangement (CPEA);

(ii) The Economy indicates its intention to make use of at least one APEC-recognized Accountability Agent subject to the procedures outlined in paragraph 6.2 of the Charter of the JOP;

(iii) The Economy's ECSG delegation, or appropriate governmental representative, after consulting with the JOP, submits to the Chair of the ECSG an explanation of how the CBPR System program requirements may be enforced in that Economy; and

(iv) The JOP submits to the Chair of the ECSG a report as to how the conditions in (i)-(iii) above have been satisfied.

The purpose of Annex B is to assist Economies and the JOP in fulfilling the requirements of items (iii) and (iv):

- *This document provides the baseline program requirements of the APEC Cross Border Privacy Rules (CBPR) System in order to guide the Economy's explanation of how each requirement may be enforced in that Economy; and*
- *The information provided by the Economy will form the basis of the JOP's report.*

Contents

NOTICE 3

COLLECTION LIMITATION 20

USES OF PERSONAL INFORMATION 27

CHOICE 43

INTEGRITY OF PERSONAL INFORMATION 83

SECURITY SAFEGUARDS 94

ACCESS AND CORRECTION 115

ACCOUNTABILITY 122

NOTICE

Assessment Purpose – *To ensure that individuals understand the applicant's personal information policies (subject to any qualifications), including to whom the personal information may be transferred and the purpose for which the personal information may be used. Refer to the APEC Cross Border Privacy Rules Intake Questionnaire for a list of acceptable Qualifications to the provision of notice.*

Question (*to be answered by the Applicant*)	Assessment Criteria (*to be verified by the Accountability Agent*)	Enforceability (*to be answered by the Economy*)
1. Do you provide clear and easily accessible statements about your practices and policies that govern the personal information described above (a privacy statement)? Where YES, provide a copy of all applicable privacy statements and/or hyperlinks to the same.	If YES, the Accountability Agent must verify that the Applicant's privacy practices and policy (or other privacy statement) include the following characteristics: • Available on the Applicant's Website, such as text on a Web page, link from URL, attached document, pop-up windows, included on frequently asked questions (FAQs), or other (must be specified). • Is in accordance with the principles of the APEC Privacy Framework; • Is easy to find and accessible. • Applies to all personal information; whether collected online or offline. • States an effective date of Privacy Statement publication. Where Applicant answers NO to question 1, and	*Privacy Act 1988 1988 – Australian Privacy Principles (APPs)* APP 1 & APP 5 APP 1 imposes three separate obligations upon an APP entity to: - take reasonable steps to implement practices, procedures and systems that will ensure the entity complies with the APPs and any binding registered APP code, and is able to deal with related inquiries and complaints (APP 1.2) - have a clearly expressed and up-to-date APP Privacy Policy about how the entity manages personal information (APP 1.3 and 1.4) - take reasonable steps to make its APP Privacy Policy available free of charge in an appropriate form (APP 1.5) and, upon request, in a particular form (APP 1.6).

	does not identify an applicable qualification subject to the Qualifications to Notice set out below, the Accountability Agent must inform the Applicant that Notice as described herein is required for compliance with this principle. Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.	APP 5 APP5 requires an APP entity that collects personal information about an individual to take reasonable steps either to notify the individual of certain matters or to ensure the individual is aware of those matters. Reasonable steps must be taken at or before the time of collection. The matters to be included in a notification include: - The APP entity's identity and contact details - Facts and circumstances of collection - If collection is required or authorised by law - The purpose of collection - Consequences for the individual if personal information is not collected - Other APP entities, bodies or persons to which the personal information is usually disclosed - Information about access and correction in the entity's Privacy Policy - Likely cross-border disclosure of personal information - When notification is to occur. The requirement to notify applies to all personal information 'collected' about an individual, either directly from the individual or from a third party.
1.a) Does this privacy statement describe how personal information is	If YES, the Accountability Agent must verify that:	APP 1 & APP 5 APP 1.3 requires an APP entity to have a clearly

collected?	• The statement describes the collection practices and policies applied to all covered personal information collected by the Applicant. • the Privacy Statement indicates what types of personal information, whether collected directly or through a third party or agent, is collected, and • The Privacy Statement reports the categories or specific sources of all categories of personal information collected. If NO, the Accountability Agent must inform the Applicant that Notice as described herein is required for compliance with this principle.	expressed and up-to-date APP Privacy Policy about how it manages personal information. APP 1.4 contains a non-exhaustive list of information that an APP entity must include in its APP Privacy Policy: - the kinds of personal information collected and held by the entity (APP 1.4(a)) - how personal information is collected and held (APP 1.4(b)) - the purposes for which personal information is collected, held, used and disclosed (APP 1.4(c)) - how an individual may access their personal information and seek its correction (APP 1.4(d)) - how an individual may complain if the entity breaches the APPs or any registered binding APP code, and how the complaint will be handled (APP 1.4(e)) - whether the entity is likely to disclose personal information to overseas recipients (APP 1.4(f)), 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 (APP 1.4(g)). APP 5 APP5 requires an APP entity that collects personal information about an individual to take reasonable steps either to notify the individual of certain matters or to ensure the individual is aware of those matters. Reasonable steps must be taken at or before the time of

		collection. The matters to be included in a notification include: - The APP entity's identity and contact details (APP 5.2(a)) - Facts and circumstances of collection (APP 5.2(b)) - If collection is required or authorised by law(APP 5.2(c)) - The purpose of collection (APP 5.2(d)) - Consequences for the individual if (APP 5.2(e)) personal information is not collected - Other APP entities, bodies or persons to which the personal information is usually disclosed (APP 5.2(f)) - Information about access and correction in the entity's Privacy Policy (APP 5.2(g)) - How the individual may complain about a breach of the APPs and how an entity will deal with such complaint (APP5.2(h)) - Likely cross-border disclosure of personal information (APP 5.2(i)) - When notification is to occur (APP 5.1) The requirement to notify applies to all personal information 'collected' about an individual, either directly from the individual or from a third party.
1.b) Does this privacy statement describe the	Where the Applicant answers YES, the Accountability Agent must verify that the	APP 1 & 5 APP 1.4 contains a non-exhaustive list of information that

purpose(s) for which personal information is collected?	Applicant provides notice to individuals of the purpose for which personal information is being collected. Where the Applicant answers NO and does not identify an applicable qualification set out below, the Accountability Agent must notify the Applicant that notice of the purposes for which personal information is collected is required and must be included in their Privacy Statement. Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.	an APP entity must include in its APP Privacy Policy: - the kinds of personal information collected and held by the entity (APP 1.4(a)) - how personal information is collected and held (APP 1.4(b)) - the purposes for which personal information is collected, held, used and disclosed (APP 1.4(c)) - how an individual may access their personal information and seek its correction (APP 1.4(d)) - how an individual may complain if the entity breaches the APPs or any registered binding APP code, and how the complaint will be handled (APP 1.4(e)) - whether the entity is likely to disclose personal information to overseas recipients (APP 1.4(f)), 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 (APP 1.4(g)). APP 5 APP5 requires an APP entity that collects personal information about an individual to take reasonable steps either to notify the individual of certain matters or to ensure the individual is aware of those matters. Reasonable steps must be taken at or before the time of collection. The matters to be included in a notification include: - The APP entity's identity and contact details (APP 5.2(a))

		- Facts and circumstances of collection (APP 5.2(b)) - If collection is required or authorised by law(APP 5.2(c)) - The purpose of collection (APP 5.2(d)) - Consequences for the individual if (APP 5.2(e)) personal information is not collected - Other APP entities, bodies or persons to which the personal information is usually disclosed (APP 5.2(f)) - Information about access and correction in the entity's Privacy Policy (APP 5.2(g)) - How the individual may complain about a breach of the APPs and how an entity will deal with such complaint (APP5.2(h)) - Likely cross-border disclosure of personal information (APP 5.2(i)) - When notification is to occur (APP 5.1) The requirement to notify applies to all personal information 'collected' about an individual, either directly from the individual or from a third party.
1.c) Does this privacy statement inform individuals whether their personal information is made available to third parties and for what purpose?	Where the Applicant answers YES, the Accountability Agent must verify that the Applicant notifies individuals that their personal information will or may be made available to third parties, identifies the categories or specific third parties, and the purpose for which the personal information will or may be made available.	APP1 and APP5 APP 1.4 contains a non-exhaustive list of information that an APP entity must include in its APP Privacy Policy: - the kinds of personal information collected and held by the entity (APP 1.4(a)) - how personal information is collected and held (APP 1.4(b))

	Where the Applicant answers NO and does not identify an applicable qualification, the Accountability Agent must notify the Applicant that notice that personal information will be available to third parties is required and must be included in their Privacy Statement. Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.	- the purposes for which personal information is collected, held, used and disclosed (APP 1.4(c)) - how an individual may access their personal information and seek its correction (APP 1.4(d)) - how an individual may complain if the entity breaches the APPs or any registered binding APP code, and how the complaint will be handled (APP 1.4(e)) - whether the entity is likely to disclose personal information to overseas recipients (APP 1.4(f)), 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 (APP 1.4(g)). APP 5 APP5 requires an APP entity that collects personal information about an individual to take reasonable steps either to notify the individual of certain matters or to ensure the individual is aware of those matters. Reasonable steps must be taken at or before the time of collection. The matters to be included in a notification include: - The APP entity's identity and contact details (APP 5.2(a)) - Facts and circumstances of collection (APP 5.2(b)) - If collection is required or authorised by law(APP 5.2(c)) - The purpose of collection (APP 5.2(d))

		- Consequences for the individual if (APP 5.2(e)) personal information is not collected - Other APP entities, bodies or persons to which the personal information is usually disclosed (APP 5.2(f)) - Information about access and correction in the entity's Privacy Policy (APP 5.2(g)) - How the individual may complain about a breach of the APPs and how an entity will deal with such complaint (APP5.2(h)) - Likely cross-border disclosure of personal information (APP 5.2(i)) - When notification is to occur (APP 5.1) The requirement to notify applies to all personal information 'collected' about an individual, either directly from the individual or from a third party.
1.d) Does this privacy statement disclose the name of the applicant's company and location, including contact information regarding practices and handling of personal information upon collection? Where YES describe.	Where the Applicant answers YES, the Accountability Agent must verify that the Applicant provides name, address and e-mail address. Where the Applicant answers NO, the Accountability Agent must inform the Applicant that such disclosure is required for compliance with this principle. Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.	APP1 & APP 5 APP 1.4 contains a non-exhaustive list of information that an APP entity must include in its APP Privacy Policy: - the kinds of personal information collected and held by the entity (APP 1.4(a)) - how personal information is collected and held (APP 1.4(b)) - the purposes for which personal information is collected, held, used and disclosed (APP 1.4(c)) - how an individual may access their personal information and seek its correction (APP 1.4(d)) - how an individual may complain if the entity breaches

	principle. Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.	- the APPs or any registered binding APP code, and how the complaint will be handled (APP 1.4(e)) - whether the entity is likely to disclose personal information to overseas recipients (APP 1.4(f)), 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 (APP 1.4(g)). APP 5 APP5 requires an APP entity that collects personal information about an individual to take reasonable steps either to notify the individual of certain matters or to ensure the individual is aware of those matters. Reasonable steps must be taken at or before the time of collection. The matters to be included in a notification include: - The APP entity's identity and contact details (APP 5.2(a)) - Facts and circumstances of collection (APP 5.2(b)) - If collection is required or authorised by law (APP 5.2(c)) - The purpose of collection (APP 5.2(d)) - Consequences for the individual if (APP 5.2(e)) personal information is not collected - Other APP entities, bodies or persons to which the personal information is usually disclosed (APP 5.2(f)) - Information about access and correction in the entity's Privacy Policy (APP 5.2(g))

		- How the individual may complain about a breach of the APPs and how an entity will deal with such complaint (APP5.2(h)) - Likely cross-border disclosure of personal information (APP 5.2(i)) - When notification is to occur (APP 5.1) The requirement to notify applies to all personal information 'collected' about an individual, either directly from the individual or from a third party.
1.e) Does this privacy statement provide information regarding the use and disclosure of an individual's personal information?	Where the Applicant answers YES, the Accountability Agent must verify that the Applicant's Privacy Statement includes, if applicable, information regarding the use and disclosure of all personal information collected. Refer to question 8 for guidance on permissible uses of personal information. Where the Applicant answers NO and does not identify an applicable qualification, the Accountability Agent must inform the Applicant, that such information is required for compliance with this principle. Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.	APP1 & APP 5 APP 1.4 contains a non-exhaustive list of information that an APP entity must include in its APP Privacy Policy: - the kinds of personal information collected and held by the entity (APP 1.4(a)) - how personal information is collected and held (APP 1.4(b)) - the purposes for which personal information is collected, held, used and disclosed (APP 1.4(c)) - how an individual may access their personal information and seek its correction (APP 1.4(d)) - how an individual may complain if the entity breaches - the APPs or any registered binding APP code, and how the complaint will be handled (APP 1.4(e)) - whether the entity is likely to disclose personal information to overseas recipients (APP 1.4(f)), 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 (APP 1.4(g)). APP5 APP5 requires an APP entity that collects personal information about an individual to take reasonable steps either to notify the individual of certain matters or to ensure the individual is aware of those matters. Reasonable steps must be taken at or before the time of collection. The matters to be included in a notification include: - The APP entity's identity and contact details (APP 5.2(a)) - Facts and circumstances of collection (APP 5.2(b)) - If collection is required or authorised by law (APP 5.2(c)) - The purpose of collection (APP 5.2(d)) - Consequences for the individual if (APP 5.2(e)) personal information is not collected - Other APP entities, bodies or persons to which the personal information is usually disclosed (APP 5.2(f)) - Information about access and correction in the entity's Privacy Policy (APP 5.2(g)) - How the individual may complain about a breach of the APPs and how an entity will deal with such complaint (APP5.2(h))

		- Likely cross-border disclosure of personal information (APP 5.2(i)) - When notification is to occur (APP 5.1) The requirement to notify applies to all personal information 'collected' about an individual, either directly from the individual or from a third party.
1.f) Does this privacy statement provide information regarding whether and how an individual can access and correct their personal information?	Where the Applicant answers YES, the Accountability Agent must verify that the Privacy Statement includes: - The process through which the individual may access his or her personal information (including electronic or traditional non-electronic means). - The process that an individual must follow in order to correct his or her personal information Where the Applicant answers NO and does not identify an applicable qualification, the Accountability Agent must inform the Applicant that providing information about access and correction, including the Applicant's typical response times for access and correction requests, is required for compliance with this principle. Where the Applicant identifies an applicable qualification, the Accountability Agent must	APP1 & APP 5 APP 1.4 contains a non-exhaustive list of information that an APP entity must include in its APP Privacy Policy: - the kinds of personal information collected and held by the entity (APP 1.4(a)) - how personal information is collected and held (APP 1.4(b)) - the purposes for which personal information is collected, held, used and disclosed (APP 1.4(c)) - how an individual may access their personal information and seek its correction (APP 1.4(d)) - how an individual may complain if the entity breaches - the APPs or any registered binding APP code, and how the complaint will be handled (APP 1.4(e)) - whether the entity is likely to disclose personal information to overseas recipients (APP 1.4(f)), 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 (APP 1.4(g)).

	verify whether the applicable qualification is justified.	APP 5 APP5 requires an APP entity that collects personal information about an individual to take reasonable steps either to notify the individual of certain matters or to ensure the individual is aware of those matters. Reasonable steps must be taken at or before the time of collection. The matters to be included in a notification include: - The APP entity's identity and contact details (APP 5.2(a)) - Facts and circumstances of collection (APP 5.2(b)) - If collection is required or authorised by law (APP 5.2(c)) - The purpose of collection (APP 5.2(d)) - Consequences for the individual if (APP 5.2(e)) personal information is not collected - Other APP entities, bodies or persons to which the personal information is usually disclosed (APP 5.2(f)) - Information about access and correction in the entity's Privacy Policy (APP 5.2(g)) - How the individual may complain about a breach of the APPs and how an entity will deal with such complaint (APP5.2(h)) - Likely cross-border disclosure of personal information (APP 5.2(i)) - When notification is to occur (APP 5.1)

		The requirement to notify applies to all personal information 'collected' about an individual, either directly from the individual or from a third party.
2. subject to the qualifications listed below, at the time of collection of personal information (whether directly or through the use of third parties acting on your behalf), do you provide notice that such information is being collected?	Where the Applicant answers YES, the Accountability Agent must verify that the Applicant provides notice to individuals that their personal information is being (or, if not practicable, has been) collected and that the notice is reasonably available to individuals. Where the Applicant answers NO and does not identify an applicable qualification, the Accountability Agent must inform the Applicant that the notice that personal information is being collected is required for compliance with this principle. Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.	APP5 APP5 requires an APP entity that collects personal information about an individual to take reasonable steps either to notify the individual of certain matters or to ensure the individual is aware of those matters. Reasonable steps must be taken at or before the time of collection. The matters to be included in a notification include: - The APP entity's identity and contact details (APP 5.2(a)) - Facts and circumstances of collection (APP 5.2(b)) - If collection is required or authorised by law (APP 5.2(c)) - The purpose of collection (APP 5.2(d)) - Consequences for the individual if (APP 5.2(e)) personal information is not collected - Other APP entities, bodies or persons to which the personal information is usually disclosed (APP 5.2(f)) - Information about access and correction in the entity's Privacy Policy (APP 5.2(g)) - How the individual may complain about a breach of the APPs and how an entity will deal with such complaint (APP5.2(h))

		- Likely cross-border disclosure of personal information (APP 5.2(i)) - When notification is to occur (APP 5.1) The requirement to notify applies to all personal information 'collected' about an individual, either directly from the individual or from a third party.
3. Subject to the qualifications listed below, at the time of collection of personal information (whether directly or through the use of third parties acting on your behalf), do you indicate the purpose(s) for which personal information is being collected?	Where the Applicant answers YES, the Accountability Agent must verify that the Applicant explains to individuals the purposes for which personal information is being collected. The purposes must be communicated orally or in writing, for example on the Applicant's website, such as text on a website link from URL, attached documents, pop-up window, or other. Where the Applicant answers NO and does not identify an applicable qualification set out on part II of the CBPR Self-Assessment Guidelines for Organisations, the Accountability Agent must inform the Applicant of the need to provide notice to individuals of the purposes for which personal information is being collected. Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.	APP5 requires an APP entity that collects personal information about an individual to take reasonable steps either to notify the individual of certain matters or to ensure the individual is aware of those matters. Reasonable steps must be taken at or before the time of collection. The matters to be included in a notification include: - The APP entity's identity and contact details (APP 5.2(a)) - Facts and circumstances of collection (APP 5.2(b)) - If collection is required or authorised by law (APP 5.2(c)) - The purpose of collection (APP 5.2(d)) - Consequences for the individual if (APP 5.2(e)) personal information is not collected - Other APP entities, bodies or persons to which the personal information is usually disclosed (APP 5.2(f)) - Information about access and correction in the entity's Privacy Policy (APP 5.2(g)) - How the individual may complain about a breach of

		the APPs and how an entity will deal with such complaint (APP5.2(h)) - Likely cross-border disclosure of personal information (APP 5.2(i)) - When notification is to occur (APP 5.1) The requirement to notify applies to all personal information 'collected' about an individual, either directly from the individual or from a third party.
4. Subject to the qualifications listed below, at the time of collection of personal information, do you notify individuals that their personal information may be shared with third parties?	Accountability Agent must verify that the Applicant provides notice to individuals that their personal information will be or may be shared with third parties and for what purposes. Where the Applicant answers NO and does not identify an applicable qualification set out on part II of the CBPR Self-Assessment Guidelines for Organisations, the Accountability Agent must inform the Applicant to provide notice to individuals that the personal information collected may be shared with third parties. Where the Applicant identifies an applicable qualification, the Accountability Agent must determine whether the applicable qualification is justified.	APP5 APP5 requires an APP entity that collects personal information about an individual to take reasonable steps either to notify the individual of certain matters or to ensure the individual is aware of those matters. Reasonable steps must be taken at or before the time of collection, or as soon as practicable afterwards. The matters to be included in a notification include: - The APP entity's identity and contact details - Facts and circumstances of collection - If collection is required or authorised by law - The purpose of collection - Consequences for the individual if personal information is not collected - Other APP entities, bodies or persons to which the personal information is usually disclosed - Information about access and correction in the entity's Privacy Policy

		- Likely cross-border disclosure of personal information - When notification is to occur. The requirement to notify applies to all personal information ‘collected’ about an individual, either directly from the individual or from a third party.

COLLECTION LIMITATION

Assessment Purpose - *Ensuring that collection of information is limited to the specific purposes stated at the time of collection. The collection of the information should be relevant to such purposes, and proportionality to the fulfillment of such purposes may be a factor in determining what is relevant. In all instances, collection methods must be lawful and fair*

Question (*to be answered by the Applicant*)	Assessment Criteria (*to be verified by the Accountability Agent*)	Enforceability (*to be answered by the Economy*)
5. How do you obtain personal information: 5.a) Directly from the individual? 5.b) From third parties collecting on your behalf? 5.c) Other. If YES, describe.	The Accountability Agent must verify that the Applicant indicates from whom they obtain personal information. Where the Applicant answers YES to any of these sub-parts, the Accountability Agent must verify the Applicant's practices in this regard. There should be at least one 'yes' answer to these three questions. If not, the Accountability Agent must inform the Applicant that it has incorrectly completed the questionnaire.	APP 1, 3, 5 APP 1.3 requires an APP entity to have a clearly expressed and up-to-date APP Privacy Policy about how it manages personal information. APP 1.4 contains a non-exhaustive list of information that an APP entity must include in its APP Privacy Policy: - the kinds of personal information collected and held by the entity (APP 1.4(a)) - how personal information is collected and held (APP 1.4(b)) - the purposes for which personal information is collected, held, used and disclosed (APP 1.4(c)) - how an individual may access their personal information and seek its correction (APP 1.4(d)) - how an individual may complain if the entity breaches the APPs or any registered binding APP code, and how the complaint will be handled (APP 1.4(e)) - whether the entity is likely to disclose personal information to overseas recipients (APP 1.4(f)), 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 (APP 1.4(g)). APP3 APP 3 deals with when an APP entity can collect personal information, and how an APP entity must collect personal information. The APPs distinguish between an APP entity collecting solicited personal information (APP 3) and receiving unsolicited personal information (APP 4). For personal information (other than sensitive information), an APP entity that is: - a government agency, may only collect this information where it is reasonably necessary for, or directly related to, the agency's functions or activities (APP 3.1) - an organisation, may only collect this information where it is reasonably necessary for the organisation's functions or activities(APP 3.2). APP 3 contains different requirements for the collection of sensitive information compared to other types of personal information. Unless an exception applies, an APP entity may only collect sensitive information where the individual concerned consents to the collection (APP 3.3).

		Personal information must only be collected by lawful and fair means (APP 3.5). Personal information must be collected from the individual concerned, unless this is unreasonable or impracticable (additional exceptions apply to government agencies) (APP 3.6). APP5 APP5 requires an APP entity that collects personal information about an individual to take reasonable steps either to notify the individual of certain matters or to ensure the individual is aware of those matters. Reasonable steps must be taken at or before the time of collection. The matters to be included in a notification include: - The APP entity's identity and contact details (APP 5.2(a)) - Facts and circumstances of collection (APP 5.2(b)) - If collection is required or authorised by law (APP 5.2(c)) - The purpose of collection (APP 5.2(d)) - Consequences for the individual if (APP 5.2(e)) personal information is not collected - Other APP entities, bodies or persons to which the personal information is usually disclosed (APP 5.2(f)) - Information about access and correction in the entity's

		Privacy Policy (APP 5.2(g)) - How the individual may complain about a breach of the APPs and how an entity will deal with such complaint (APP5.2(h)) - Likely cross-border disclosure of personal information (APP 5.2(i)) - When notification is to occur (APP 5.1) The requirement to notify applies to all personal information 'collected' about an individual, either directly from the individual or from a third party.
6. Do you limit your personal information collection (whether directly or through the use of third parties acting on your behalf) to information that is relevant to fulfill the purpose(s) for which it is collected or other compatible or related purposes?	Where the Applicant answers YES and indicates it only collects personal information which is relevant to the identified collection purpose or other compatible or related purposes, the Accountability Agent must require the Applicant to identify: □ Each type of data collected □ The corresponding stated purpose of collection for each; and □ All uses that apply to each type of data □ An explanation of the compatibility or relatedness of each identified use with the stated purpose of collection	APP3 The APPs distinguish between an APP entity collecting solicited personal information (APP 3) and receiving unsolicited personal information (APP 4). APP 3 deals with when an APP entity can collect personal information, and how an APP entity must collect personal information. For personal information (other than sensitive information), an APP entity that is: - A government agency, may only collect this information where it is reasonably necessary for, or directly related to, the agency's functions or activities (APP 3.1)

	Using the above, the Accountability Agent will verify that the applicant limits the amount and type of personal information to that which is relevant to fulfill the stated purposes Where the Applicant answers NO, the Accountability Agent must inform the Applicant that it must limit the use of collected personal information to those uses that are relevant to fulfilling the purpose(s) for which it is collected.	- an organisation, may only collect this information where it is reasonably necessary for the organisation's functions or activities(APP 3.2). APP 3 contains different requirements for the collection of sensitive information compared to other types of personal information. Unless an exception applies, an APP entity may only collect sensitive information where the individual concerned consents to the collection (APP 3.3). Personal information must only be collected by lawful and fair means (APP 3.5). Personal information must be collected from the individual concerned, unless this is unreasonable or impracticable (additional exceptions apply to government agencies) (APP 3.6).
7. Do you collect personal information (whether directly or through the use of third parties acting on your behalf) by lawful and fair means, consistent with the requirements of the jurisdiction that governs the collection of such personal information? Where YES, describe.	Where the Applicant answers YES, the Accountability Agent must require the Applicant to certify that it is aware of and complying with the requirements of the jurisdiction that governs the collection of such personal information and that it is collecting information by fair means, without deception.	APP1, 3 APP 1 requires an APP entity to: - take reasonable steps to implement practices, procedures and systems that will ensure the entity complies with the APPs and any binding registered APP code, and is able to deal with related inquiries and complaints (APP 1.2)

	Where the Applicant Answers NO, the Accountability Agent must inform that Applicant that lawful and fair procedures are required for compliance with this principle.	- have a clearly expressed and up-to-date APP Privacy Policy about how the entity manages personal information (APP 1.3 and 1.4) - take reasonable steps to make its APP Privacy Policy available free of charge in an appropriate form (APP 1.5) and, upon request, in a particular form (APP 1.6). APP3 The APPs distinguish between an APP entity collecting solicited personal information (APP 3) and receiving unsolicited personal information (APP 4). APP 3 deals with when an APP entity can collect personal information, and how an APP entity must collect personal information. For personal information (other than sensitive information), an APP entity that is: - a government agency, may only collect this information where it is reasonably necessary for, or directly related to, the agency's functions or activities (APP 3.1) - an organisation, may only collect this information where it is reasonably necessary for the organisation's functions or activities(APP 3.2). APP 3 contains different requirements for the collection

		of sensitive information compared to other types of personal information. Unless an exception applies, an APP entity may only collect sensitive information where the individual concerned consents to the collection (APP 3.3). Personal information must only be collected by lawful and fair means (APP 3.5). Personal information must be collected from the individual concerned, unless this is unreasonable or impracticable (additional exceptions apply to government agencies) (APP 3.6).

USES OF PERSONAL INFORMATION

Assessment Purpose - *Ensuring that the use of personal information is limited to fulfilling the specific purposes of collection and other compatible or related purposes. This section covers use, transfer and disclosure of personal information. Application of this Principle requires consideration of the nature of the information, the context of collection and the intended use of the information. The fundamental criterion in determining whether a purpose is compatible with or related to the stated purposes is whether the extended usage stems from or is in furtherance of such purposes. The use of personal information for "compatible or related purposes" could extend, for example, to matters such as the creation and use of a centralized database to manage personnel in an effective and efficient manner; the processing of employee payrolls by a third party; or, the use of information collected by an applicant for the purpose of granting credit for the subsequent purpose of collecting debt owed to that applicant.*

Question (*to be answered by the Applicant*)	Assessment Criteria (*to be verified by the Accountability Agent*)	Enforceability (*to be answered by the Economy*)
8. Do you limit the use of the personal information you collect (whether directly or through the use of third parties acting on your behalf) as identified in your privacy statement and/or in the notice provided at the time of collection, to those purposes for which the information was collected or for other compatible or related purposes? If necessary, provide a description in the space below.	Where the Applicant answers YES, the Accountability Agent must verify the existence of written policies and procedures to ensure that] all covered personal information collected either directly or indirectly through an agent is done so in accordance with the purposes for which the information was collected as identified in the Applicant's Privacy Statement(s) in effect at the time of collection or for other compatible or related purposes. Where the Applicant Answers NO, the Accountability Agent must consider answers to Question 9 below.	APP 6 APP 6 outlines when an APP entity may use or disclose personal information. An APP entity can only use or disclose personal information for a purpose for which it was collected (known as the 'primary purpose'), or for a secondary purpose if an exception applies. The exceptions include where: - the individual has consented to a secondary use or disclosure (APP6.1(a)) - the individual would reasonably expect the APP entity to use or disclose their personal information for the secondary purpose, and that purpose is related to the primary purpose of collection, or, in the case of sensitive information, directly related to the primary

		purpose (APP6.2(a)). - the secondary use or disclosure is required or authorised by or under an Australian law or a court/tribunal order (APP6.2(b)) - a permitted general situation exists in relation to the secondary use or disclosure (APP6.2(c)) - the APP entity is an organisation and a permitted health situation exists in relation to the secondary use or disclosure (APP6.2(d)) - the APP entity reasonably believes that the secondary use or disclosure is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body,(APP6.2(e)) or - the APP entity is a government agency (other than an enforcement body) and discloses biometric information or biometric templates to an enforcement body, and the disclosure is conducted in accordance with guidelines made by the Information Commissioner for the purposes of APP 6.3 (APP6.3). An APP entity may disclose personal information, other than sensitive information, to a related body corporate (s 13B(1)(b)).

		APP 6 does not apply to the use or disclosure by an organisation of: - personal information for the purpose of direct marketing (this is covered by APP 7), or - government related identifiers (this is covered by APP 9) (APP 6.7). APP7 Although APP7 does not explicitly limit secondary uses, in practice it may provide an additional protection to that provided under APP 6, by preventing the use of personal information for a secondary use (which is specifically for direct marketing), where the information was collected for another purpose. APP 7 provides that an organisation must not use or disclose personal information it holds for the purpose of direct marketing unless an exception applies (APP 7.1). The exceptions in APP 7.2 and 7.3 apply to personal information other than sensitive information. They draw a distinction between the use or disclosure of personal information by an organisation where: - the personal information has been collected directly from an individual, and the individual

		would reasonably expect their personal information to be used for the purpose of direct marketing (APP 7.2), and - the personal information has been collected from a third party, or from the individual directly but the individual does not have a reasonable expectation that their personal information will be used for the purpose of direct marketing (APP 7.3). Sources of third party data include data list providers, third party mobile applications, third party lead generation and enhancement data. Exceptions to this principle also apply in relation to: - sensitive information (APP 7.4), and - an organisation that is a contracted service provider for a Commonwealth contract (APP 7.5). APP 7 does not apply to the extent that the *Do Not Call Register Act 2006*, the *Spam Act 2003* or any other legislation prescribed by the regulations apply (APP 7.8). APP 7 will still apply to the acts or practices of an organisation that are exempt from these Acts. An individual may request an organisation not to use or disclose their personal information for the purpose of direct marketing, or for the purpose of

		facilitating direct marketing by other organisations (APP 7.6). The organisation must give effect to any such request by an individual within a reasonable period of time and for free (APP 7.7). An organisation must, on request, notify an individual of its source of the individual's personal information that it has used or disclosed for the purpose of direct marketing unless this is unreasonable or impracticable to do so (APP 7.6).
9. If you answered NO, do you use the personal information you collect for unrelated purposes under one of the following circumstances? Describe below. 9.a) Based on express consent of the individual? 9.b) Compelled by applicable laws?	Where the Applicant answers NO to question 8, the Applicant must clarify under what circumstances it uses personal information for purposes unrelated to the purposes of collection and specify those purposes. Where the applicant selects 9a, the Accountability Agent must verify that the Applicant's use of the personal information is based on express consent of the individual (9.a), such as: □ Online at point of collection □ Via e-mail □ Via preference/profile page □ Via telephone □ Via postal mail, or □ Other (in case, specify)	*Privacy Act 1988* The Privacy Act defines 'consent' as 'express consent or implied consent'(s6). It also makes special provision for 'sensitive information' which is a sub-category of personal information and may include personal information about an individual's racial or ethnic origin, political opinions, religion or sexual orientation. An APP entity will generally be required to seek express consent before handling 'sensitive information', given the greater impact on privacy the use of this information may have. How the CBPR program requirements for express consent interact with the APPs may require further consideration under the proposed Code, which is to be developed pursuant to Part IIIB of the Privacy Act.

	Where the Applicant answers 9.a, the Accountability Agent must require the Applicant to provide a description of how such consent was obtained. The consent must meet the requirements set forth in questions 17-19 below. Where the Applicant selects 9.b, the Accountability Agent must require the Applicant to provide a description of how the collected personal information may be shared, used or disclosed as compelled by law. Where the Applicant does not answer 9.a or 9.b, the Accountability Agent must inform the Applicant that limiting the use of collected information to the identified purposes of collection or other compatible or related purposes, unless permitted under the circumstances listed in this Question, is required for compliance with this principle.	APP 6 - APP 6 outlines when an APP entity may use or disclose personal information. An APP entity can only use or disclose personal information for a purpose for which it was collected (known as the 'primary purpose'), or for a secondary purpose if an exception applies. The exceptions include where: - the individual has consented to a secondary use or disclosure (APP6.1(a)) - the individual would reasonably expect the APP entity to use or disclose their personal information for the secondary purpose, and that purpose is related to the primary purpose of collection, or, in the case of sensitive information, directly related to the primary purpose (APP6.2(a)). - the secondary use or disclosure is required or authorised by or under an Australian law or a court/tribunal order (APP6.2(b)) - a permitted general situation exists in relation to the secondary use or disclosure (APP6.2(c)) - the APP entity is an organisation and a permitted health situation exists in relation to the secondary use or disclosure (APP6.2(d)) - the APP entity reasonably believes that the

		secondary use or disclosure is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body,(APP6.2(e)) or - the APP entity is a government agency (other than an enforcement body) and discloses biometric information or biometric templates to an enforcement body, and the disclosure is conducted in accordance with guidelines made by the Information Commissioner for the purposes of APP 6.3 (APP6.3). An APP entity may disclose personal information, other than sensitive information, to a related body corporate (s 13B(1)(b)). APP 6 does not apply to the use or disclosure by an organisation of: - personal information for the purpose of direct marketing (this is covered by APP 7), or - government related identifiers (this is covered by APP 9) (APP 6.7). APP7 Although APP7 does not explicitly limit secondary uses, in practice it may provide an additional protection to that provided under APP 6, by

		preventing the use of personal information for a secondary use (which is specifically for direct marketing), where the information was collected for another purpose. APP 7 provides that an organisation must not use or disclose personal information it holds for the purpose of direct marketing unless an exception applies (APP 7.1). The exceptions in APP 7.2 and 7.3 apply to personal information other than sensitive information. They draw a distinction between the use or disclosure of personal information by an organisation where: - the personal information has been collected directly from an individual, and the individual would reasonably expect their personal information to be used for the purpose of direct marketing (APP 7.2), and - the personal information has been collected from a third party, or from the individual directly but the individual does not have a reasonable expectation that their personal information will be used for the purpose of direct marketing (APP 7.3). Sources of third party data include data list providers, third party mobile applications, third

		party lead generation and enhancement data. Exceptions to this principle also apply in relation to: - sensitive information (APP 7.4), and - an organisation that is a contracted service provider for a Commonwealth contract (APP 7.5). APP 7 does not apply to the extent that the *Do Not Call Register Act 2006*, the *Spam Act 2003* or any other legislation prescribed by the regulations apply (APP 7.8). APP 7 will still apply to the acts or practices of an organisation that are exempt from these Acts. An individual may request an organisation not to use or disclose their personal information for the purpose of direct marketing, or for the purpose of facilitating direct marketing by other organisations (APP 7.6). The organisation must give effect to any such request by an individual within a reasonable period of time and for free (APP 7.7). An organisation must, on request, notify an individual of its source of the individual's personal information that it has used or disclosed for the purpose of direct marketing unless this is unreasonable or impracticable to do so (APP 7.6).

10. Do you disclose personal information you collect (whether directly or through the use of third parties acting on your behalf) to other personal information controllers? If YES, describe.	Where the Applicant answers YES in questions 10 and 11, the Accountability Agent must verify that if personal information is disclosed to other personal information controllers or transferred to processors, such disclosure and/or transfer must be undertaken to fulfill the original purpose of collection or another compatible or related purpose, unless based upon the express consent of the individual necessary to provide a service or product requested by the individual, or compelled by law. Also, the Accountability Agent must require the Applicant to identify: 1) each type of data disclosed or transferred; 2) the corresponding stated purpose of collection for each type of disclosed data; and 3) the manner in which the disclosure fulfills the identified purpose (e.g. order fulfillment etc.). Using the above, the Accountability Agent must verify that the Applicant's disclosures or transfers of all personal information is limited to the purpose(s) of collection, or	APP1, 5, 6 APP 1.4 contains a non-exhaustive list of information that an APP entity must include in its APP Privacy Policy: - the kinds of personal information collected and held by the entity (APP 1.4(a)) - how personal information is collected and held (APP 1.4(b)) - the purposes for which personal information is collected, held, used and disclosed (APP 1.4(c)) - how an individual may access their personal information and seek its correction (APP 1.4(d)) - how an individual may complain if the entity breaches the APPs or any registered binding APP code, and how the complaint will be handled (APP 1.4(e)) - whether the entity is likely to disclose personal information to overseas recipients (APP 1.4(f)), 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 (APP 1.4(g)). APP5 APP5 requires an APP entity that collects personal information about an individual to take reasonable

	compatible or related purposes.	steps either to notify the individual of certain matters or to ensure the individual is aware of those matters. Reasonable steps must be taken at or before the time of collection. The matters to be included in a notification include: - The APP entity's identity and contact details (APP 5.2(a)) - Facts and circumstances of collection (APP 5.2(b)) - If collection is required or authorised by law (APP 5.2(c)) - The purpose of collection (APP 5.2(d)) - Consequences for the individual if (APP 5.2(e)) personal information is not collected - Other APP entities, bodies or persons to which the personal information is usually disclosed (APP 5.2(f)) - Information about access and correction in the entity's Privacy Policy (APP 5.2(g)) - How the individual may complain about a breach of the APPs and how an entity will deal with such complaint (APP5.2(h)) - Likely cross-border disclosure of personal information (APP 5.2(i))

		- When notification is to occur (APP 5.1) The requirement to notify applies to all personal information 'collected' about an individual, either directly from the individual or from a third party. APP 6 APP 6 outlines when an APP entity may use or disclose personal information. An APP entity can only use or disclose personal information for a purpose for which it was collected (known as the 'primary purpose'), or for a secondary purpose if an exception applies. The exceptions include where: - the individual has consented to a secondary use or disclosure (APP6.1(a)) - the individual would reasonably expect the APP entity to use or disclose their personal information for the secondary purpose, and that purpose is related to the primary purpose of collection, or, in the case of sensitive information, directly related to the primary purpose (APP6.2(a)). - the secondary use or disclosure is required or authorised by or under an Australian law or a court/tribunal order (APP6.2(b)) - a permitted general situation exists in relation to the secondary use or disclosure (APP6.2(c))

		- the APP entity is an organisation and a permitted health situation exists in relation to the secondary use or disclosure (APP6.2(d)) - the APP entity reasonably believes that the secondary use or disclosure is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body,(APP6.2(e)) or - the APP entity is a government agency (other than an enforcement body) and discloses biometric information or biometric templates to an enforcement body, and the disclosure is conducted in accordance with guidelines made by the Information Commissioner for the purposes of APP 6.3 (APP6.3). An APP entity may disclose personal information, other than sensitive information, to a related body corporate (s 13B(1)(b)). APP 6 does not apply to the use or disclosure by an organisation of: - personal information for the purpose of direct marketing (this is covered by APP 7), or - government related identifiers (this is covered by APP 9) (APP 6.7).

11. Do you transfer personal information to personal information processors? If YES, describe.	Ditto for Q10	See answer to Q10
12. If you answered YES to question 10 and/or question 11, is the disclosure and/or transfer undertaken to fulfill the original purpose of collection or another compatible or related purpose? If YES, describe.	Ditto for Q10	See answer to Q10
13. If you answered NO to question 12 or if otherwise appropriate, does the disclosure and/or transfer take place under one of the following circumstances? 13.a) Based on express consent of the individual? 13.b) Necessary to provide a service or product requested by the individual?	Where applicant answers NO to question 13, the Applicant must clarify under what circumstances it discloses or transfers personal information for unrelated purposes, specify those purposes. Where the Applicant answers YES to 13.a, the Accountability Agent must require the Applicant to provide a description of how individual's provide consent to having their personal information disclosed and/or transferred for an unrelated use, such as: □ Online at point of collection □ Via e-mail □ Via preference/profile page	*Privacy Act 1988* The Privacy Act defines 'consent' as 'express consent' or 'implied consent' (s6). It also makes special provision for 'sensitive information' which is a sub-category of personal information and may include personal information about an individual's racial or ethnic origin, political opinions, religion or sexual orientation. An APP entity will generally be required to seek express consent before handling 'sensitive information', given the greater impact on privacy the use of this information may have. How the CBPR program requirements for express consent interact with the APPs may require further consideration under the proposed Code, which is to be developed pursuant to Part IIIB of the Privacy Act.

	□ Via telephone □ Via postal mail, or □ Other (in case, specify) Where the Applicant answers YES to 13.b, the Accountability Agent must require the Applicant to provide a description of how the disclosure and/or transfer of collected personal information is necessary to provide a service or product requested by the individual. The Accountability Agent must verify that the disclosure or transfer is necessary to provide a service or product requested by the individual. Where the Applicant answers YES to 13.c, the Accountability Agent must require the Applicant to provide a description of how collected information may be shared, used or disclosed as compelled by law. The Applicant must also outline the legal requirements under which it is compelled to share the personal information, unless the Applicant is bound by confidentiality requirements. The Accountability Agent must verify the existence and applicability of the legal requirement.	APP 6 APP 6 outlines when an APP entity may use or disclose personal information. An APP entity can only use or disclose personal information for a purpose for which it was collected (known as the 'primary purpose'), or for a secondary purpose if an exception applies. The exceptions include where: - the individual has consented to a secondary use or disclosure (APP6.1(a)) - the individual would reasonably expect the APP entity to use or disclose their personal information for the secondary purpose, and that purpose is related to the primary purpose of collection, or, in the case of sensitive information, directly related to the primary purpose (APP6.2(a)). - the secondary use or disclosure is required or authorised by or under an Australian law or a court/tribunal order (APP6.2(b)) - a permitted general situation exists in relation to the secondary use or disclosure (APP6.2(c)) - the APP entity is an organisation and a permitted health situation exists in relation to the secondary use or disclosure (APP6.2(d)) - the APP entity reasonably believes that the

	Where the Applicant answers NO to 13.a, b and c, the Accountability Agent must inform the Applicant that limiting the disclosure and/or transfer of collected information to the identified purposes of collection or other compatible or related purposes, unless permitted under the circumstances listed in this Question, is required for compliance with this principle.	secondary use or disclosure is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body,(APP6.2(e)) or - the APP entity is a government agency (other than an enforcement body) and discloses biometric information or biometric templates to an enforcement body, and the disclosure is conducted in accordance with guidelines made by the Information Commissioner for the purposes of APP 6.3 (APP6.3). An APP entity may disclose personal information, other than sensitive information, to a related body corporate (s 13B(1)(b)). APP 6 does not apply to the use or disclosure by an organisation of: - personal information for the purpose of direct marketing (this is covered by APP 7), or - government related identifiers (this is covered by APP 9) (APP 6.7).

CHOICE

Assessment Purpose - *Ensuring that individuals are provided with choice in relation to collection, use, and disclosure of their personal information. However, this Principle recognizes, through the introductory words "where appropriate" in the Framework itself, that there are certain situations where consent may be clearly implied or where it would not be necessary to provide a mechanism to exercise choice. These situations are detailed in part II of the CBPR Self-Assessment Guidelines for Organisations. Refer to the APEC Cross Border Privacy Rules Intake Questionnaire for a list of acceptable Qualifications to the provision of choice mechanisms.*

Question (*to be answered by the Applicant*)	Assessment Criteria (*to be verified by the Accountability Agent*)	Enforceability (*to be answered by the Economy*
14. Subject to the qualifications described below, do you provide a mechanism for individuals to exercise choice in relation to the collection of their personal information? Where YES describe such mechanisms below.	Where the Applicant answers YES, the Accountability Agent must verify that the Applicant provides a description of the mechanisms provided to individuals so that they may exercise choice in relation to the collection of their personal information, such as: □ Online at point of collection □ Via e-mail □ Via preference/profile page □ Via telephone □ Via postal mail, or □ Other (in case, specify) The Accountability Agent must verify that these mechanisms are in place and operational and that the purpose of	The APPs are not written using the language of 'choice', but rather require entities to seek consent or fall within specified exceptions if they wish to use or disclose personal information for secondary purposes. The alignment of CBPR requirements for collection, use and disclosure of personal information under this heading will require further consideration during development of the proposed APP code (pursuant to Part IIIB of the Privacy Act). APP 1, 2, 5 & 6 APP1 APP 1.3 requires an APP entity to have a clearly expressed and up-to-date APP Privacy Policy about how it manages personal information.

	collection is clearly stated. Where the Applicant answers NO, the Applicant must identify the applicable qualification and the Accountability Agent must verify whether the applicable qualification is justified. Where the Applicant answers NO and does not identify an applicable qualification the Accountability Agent must inform the Applicant that a mechanism for individuals to exercise choice in relation to the collection of their personal information must be provided.	APP 1.4 contains a non-exhaustive list of information that an APP entity must include in its APP Privacy Policy: - the kinds of personal information collected and held by the entity (APP 1.4(a)) - how personal information is collected and held (APP 1.4(b)) - the purposes for which personal information is collected, held, used and disclosed (APP 1.4(c)) - how an individual may access their personal information and seek its correction (APP 1.4(d)) - how an individual may complain if the entity breaches the APPs or any registered binding APP code, and how the complaint will be handled (APP 1.4(e)) - whether the entity is likely to disclose personal information to overseas recipients (APP 1.4(f)), 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 (APP 1.4(g)). APP2 APP 2 provides that 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.

		That principle does not apply in relation to a particular matter if: - 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 (APP 2.2(a)), or - it is impracticable for the APP entity to deal with individuals who have not identified themselves or used a pseudonym (APP 2.2(b)). APP5 APP5 requires an APP entity that collects personal information about an individual to take reasonable steps either to notify the individual of certain matters or to ensure the individual is aware of those matters. Reasonable steps must be taken at or before the time of collection. The matters to be included in a notification include: - The APP entity's identity and contact details (APP 5.2(a)) - Facts and circumstances of collection (APP 5.2(b)) - If collection is required or authorised by law (APP 5.2(c))

		- The purpose of collection (APP 5.2(d)) - Consequences for the individual if (APP 5.2(e)) personal information is not collected - Other APP entities, bodies or persons to which the personal information is usually disclosed (APP 5.2(f)) - Information about access and correction in the entity's Privacy Policy (APP 5.2(g)) - How the individual may complain about a breach of the APPs and how an entity will deal with such complaint (APP5.2(h)) - Likely cross-border disclosure of personal information (APP 5.2(i)) - When notification is to occur (APP 5.1) The requirement to notify applies to all personal information 'collected' about an individual, either directly from the individual or from a third party. APP6 APP 6 outlines when an APP entity may use or disclose personal information. An APP entity can only use or disclose personal information for a purpose for which it was collected (known as the 'primary purpose'), or for a secondary purpose if an exception applies. The exceptions include where:

		- the individual has consented to a secondary use or disclosure (APP6.1(a)) - the individual would reasonably expect the APP entity to use or disclose their personal information for the secondary purpose, and that purpose is related to the primary purpose of collection, or, in the case of sensitive information, directly related to the primary purpose (APP6.2(a)). - the secondary use or disclosure is required or authorised by or under an Australian law or a court/tribunal order (APP6.2(b)) - a permitted general situation exists in relation to the secondary use or disclosure (APP6.2(c)) - the APP entity is an organisation and a permitted health situation exists in relation to the secondary use or disclosure (APP6.2(d)) - the APP entity reasonably believes that the secondary use or disclosure is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body,(APP6.2(e)) or - the APP entity is a government agency (other than an enforcement body) and discloses biometric information or biometric templates to an enforcement body, and the disclosure is conducted in accordance with guidelines made by the

		Information Commissioner for the purposes of APP 6.3 (APP6.3). An APP entity may disclose personal information, other than sensitive information, to a related body corporate (s 13B(1)(b)). APP 6 does not apply to the use or disclosure by an organisation of: - personal information for the purpose of direct marketing (this is covered by APP 7), or - government related identifiers (this is covered by APP 9) (APP 6.7).
15. Subject to the qualifications described below, do you provide a mechanism for individuals to exercise choice in relation to the use of their personal information? Where YES describe such mechanisms below.	Where the Applicant answers YES, the Accountability Agent must verify that the Applicant provides a description of mechanisms provided to individuals so that they may exercise choice in relation to the use of their personal information, such as: - Online at point of collection - Via e-mail - Via preference/profile page - Via telephone - Via postal mail, or - Other (in case, specify)	APP 1, 5, 6 & 7 APP1 APP 1.3 requires an APP entity to have a clearly expressed and up-to-date APP Privacy Policy about how it manages personal information. APP 1.4 contains a non-exhaustive list of information that an APP entity must include in its APP Privacy Policy: - the kinds of personal information collected and held by the entity (APP 1.4(a)) - how personal information is collected and held (APP 1.4(b))

	The Accountability Agent must verify that these types of mechanisms are in place and operational and identify the purpose(s) for which the information will be used. Subject to the qualifications outlined below, the opportunity to exercise choice should be provided to the individual at the time of collection, for subsequent uses of personal information. Subject to the qualifications outlined below, the opportunity to exercise choice may be provided to the individual after collection, but before:] - being able to make use of the personal information, when the purposes of such use is not related or compatible to the purpose for which the information was collected, and - Personal information may be disclosed or distributed to third parties, other than Service Providers. Where the Applicant answers NO, the Applicant must identify the applicable qualification to the provision of choice, and provide a description and the	- the purposes for which personal information is collected, held, used and disclosed (APP 1.4(c)) - how an individual may access their personal information and seek its correction (APP 1.4(d)) - how an individual may complain if the entity breaches the APPs or any registered binding APP code, and how the complaint will be handled (APP 1.4(e)) - whether the entity is likely to disclose personal information to overseas recipients (APP 1.4(f)), 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 (APP 1.4(g)). APP5 APP5 requires an APP entity that collects personal information about an individual to take reasonable steps either to notify the individual of certain matters or to ensure the individual is aware of those matters. Reasonable steps must be taken at or before the time of collection. The matters to be included in a notification include: - The APP entity's identity and contact details (APP 5.2(a)) - Facts and circumstances of collection (APP 5.2(b))

	Accountability Agent must verify whether the applicable qualification is justified. Where the Applicant answers NO and does not identify an acceptable qualification, the Accountability Agent must inform the Applicant a mechanism for individuals to exercise choice in relation to the use of their personal information must be provided.	- If collection is required or authorised by law (APP 5.2(c)) - The purpose of collection (APP 5.2(d)) - Consequences for the individual if (APP 5.2(e)) personal information is not collected - Other APP entities, bodies or persons to which the personal information is usually disclosed (APP 5.2(f)) - Information about access and correction in the entity's Privacy Policy (APP 5.2(g)) - How the individual may complain about a breach of the APPs and how an entity will deal with such complaint (APP5.2(h)) - Likely cross-border disclosure of personal information (APP 5.2(i)) - When notification is to occur (APP 5.1) The requirement to notify applies to all personal information 'collected' about an individual, either directly from the individual or from a third party. APP6 APP 6 outlines when an APP entity may use or disclose personal information. An APP entity can only use or disclose personal information for a purpose for which it was collected (known as the

		'primary purpose'), or for a secondary purpose if an exception applies. The exceptions include where: - the individual has consented to a secondary use or disclosure (APP6.1(a)) - the individual would reasonably expect the APP entity to use or disclose their personal information for the secondary purpose, and that purpose is related to the primary purpose of collection, or, in the case of sensitive information, directly related to the primary purpose (APP6.2(a)). - the secondary use or disclosure is required or authorised by or under an Australian law or a court/tribunal order (APP6.2(b)) - a permitted general situation exists in relation to the secondary use or disclosure (APP6.2(c)) - the APP entity is an organisation and a permitted health situation exists in relation to the secondary use or disclosure (APP6.2(d)) - the APP entity reasonably believes that the secondary use or disclosure is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body,(APP6.2(e)) or - the APP entity is a government agency (other than an enforcement body) and discloses biometric information or biometric templates to an

		enforcement body, and the disclosure is conducted in accordance with guidelines made by the Information Commissioner for the purposes of APP 6.3 (APP6.3). An APP entity may disclose personal information, other than sensitive information, to a related body corporate (s 13B(1)(b)). APP 6 does not apply to the use or disclosure by an organisation of: - personal information for the purpose of direct marketing (this is covered by APP 7), or - government related identifiers (this is covered by APP 9) (APP 6.7). APP7 APP 7 provides that an organisation must not use or disclose personal information it holds for the purpose of direct marketing unless an exception applies (APP 7.1). The exceptions in APP 7.2 and 7.3 apply to personal information other than sensitive information. They draw a distinction between the use or disclosure of personal information by an organisation where:

		- the personal information has been collected directly from an individual, and the individual would reasonably expect their personal information to be used for the purpose of direct marketing (APP 7.2), and - the personal information has been collected from a third party, or from the individual directly but the individual does not have a reasonable expectation that their personal information will be used for the purpose of direct marketing (APP 7.3). Sources of third party data include data list providers, third party mobile applications, third party lead generation and enhancement data. Exceptions to this principle also apply in relation to: - sensitive information (APP 7.4), and - an organisation that is a contracted service provider for a Commonwealth contract (APP 7.5). An individual may request an organisation not to use or disclose their personal information for the purpose of direct marketing, or for the purpose of facilitating direct marketing by other organisations (APP 7.6). The organisation must give effect to any such request by an individual within a reasonable period of time and for free (APP 7.7). An organisation must, on request, notify an

		individual of its source of the individual's personal information that it has used or disclosed for the purpose of direct marketing unless this is unreasonable or impracticable to do so (APP 7.6).
16. Subject to the qualifications described below, do you provide a mechanism for individuals to exercise choice in relation to the disclosure of their personal information? Where YES describe such mechanisms below.	Where the Applicant answers YES, the Accountability Agent must verify that the Applicant provides a description of how individuals may exercise choice in relation to the disclosure of their personal information, such as: - Online at point of collection - Via e-mail - Via preference/profile page - Via telephone - Via postal mail, or - Other (in case, specify) The Accountability Agent must verify that these types of mechanisms are in place and operational and identify the purpose(s) for which the information will be disclosed. Subject to the qualifications outlined below, the opportunity to exercise choice should be provided to the individual at the time of collection, for subsequent disclosures of personal information. Subject to the qualifications outlined below, the	APP 1, 5, 6 & 7 APP1 APP 1.3 requires an APP entity to have a clearly expressed and up-to-date APP Privacy Policy about how it manages personal information. APP 1.4 contains a non-exhaustive list of information that an APP entity must include in its APP Privacy Policy: - the kinds of personal information collected and held by the entity (APP 1.4(a)) - how personal information is collected and held (APP 1.4(b)) - the purposes for which personal information is collected, held, used and disclosed (APP 1.4(c)) - how an individual may access their personal information and seek its correction (APP 1.4(d)) - how an individual may complain if the entity breaches the APPs or any registered binding APP code, and how the complaint will be handled (APP 1.4(e)) - whether the entity is likely to disclose personal

	opportunity to exercise choice may be provided to the individual after collection, but before: - disclosing the personal information to third parties, other than Service Providers, for a purpose that is not related or when the Accountability Agent finds that the Applicant's choice mechanism is not displayed in a clear and conspicuous manner , or compatible with that for which the information was collected.] Where the Applicant answers NO, the Applicant must identify the applicable qualification to the provision of choice and provide a description and the Accountability Agent must verify whether the applicable qualification is justified. Where the Applicant answers NO and does not identify an acceptable qualification, the Accountability Agent must inform the Applicant that a mechanism for individuals to exercise choice in relation to the disclosure of their personal information must be provided.	information to overseas recipients (APP 1.4(f)), 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 (APP 1.4(g)). APP5 APP5 requires an APP entity that collects personal information about an individual to take reasonable steps either to notify the individual of certain matters or to ensure the individual is aware of those matters. Reasonable steps must be taken at or before the time of collection. The matters to be included in a notification include: - The APP entity's identity and contact details (APP 5.2(a)) - Facts and circumstances of collection (APP 5.2(b)) - If collection is required or authorised by law (APP 5.2(c)) - The purpose of collection (APP 5.2(d)) - Consequences for the individual if (APP 5.2(e)) personal information is not collected - Other APP entities, bodies or persons to which the personal information is usually disclosed (APP 5.2(f)) - Information about access and correction in the

		entity's Privacy Policy (APP 5.2(g)) - How the individual may complain about a breach of the APPs and how an entity will deal with such complaint (APP5.2(h)) - Likely cross-border disclosure of personal information (APP 5.2(i)) - When notification is to occur (APP 5.1) The requirement to notify applies to all personal information 'collected' about an individual, either directly from the individual or from a third party. APP6 APP 6 outlines when an APP entity may use or disclose personal information. An APP entity can only use or disclose personal information for a purpose for which it was collected (known as the 'primary purpose'), or for a secondary purpose if an exception applies. The exceptions include where: - the individual has consented to a secondary use or disclosure (APP6.1(a)) - the individual would reasonably expect the APP entity to use or disclose their personal information for the secondary purpose, and that purpose is related to the primary purpose of collection, or, in the case of sensitive information, directly related to the primary purpose (APP6.2(a)).

		- the secondary use or disclosure is required or authorised by or under an Australian law or a court/tribunal order (APP6.2(b)) - a permitted general situation exists in relation to the secondary use or disclosure (APP6.2(c)) - the APP entity is an organisation and a permitted health situation exists in relation to the secondary use or disclosure (APP6.2(d)) - the APP entity reasonably believes that the secondary use or disclosure is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body,(APP6.2(e)) or - the APP entity is a government agency (other than an enforcement body) and discloses biometric information or biometric templates to an enforcement body, and the disclosure is conducted in accordance with guidelines made by the Information Commissioner for the purposes of APP 6.3 (APP6.3). An APP entity may disclose personal information, other than sensitive information, to a related body corporate (s 13B(1)(b)). APP 6 does not apply to the use or disclosure by an organisation of:

		- personal information for the purpose of direct marketing (this is covered by APP 7), or - government related identifiers (this is covered by APP 9) (APP 6.7). APP7 APP 7 provides that an organisation must not use or disclose personal information it holds for the purpose of direct marketing unless an exception applies (APP 7.1). The exceptions in APP 7.2 and 7.3 apply to personal information other than sensitive information. They draw a distinction between the use or disclosure of personal information by an organisation where: - the personal information has been collected directly from an individual, and the individual would reasonably expect their personal information to be used for the purpose of direct marketing (APP 7.2), and - the personal information has been collected from a third party, or from the individual directly but the individual does not have a reasonable expectation that their personal information will be used for the purpose of direct marketing (APP 7.3). Sources of third party data include data list providers, third party mobile applications, third

		party lead generation and enhancement data. Exceptions to this principle also apply in relation to: - sensitive information (APP 7.4), and - an organisation that is a contracted service provider for a Commonwealth contract (APP 7.5). An individual may request an organisation not to use or disclose their personal information for the purpose of direct marketing, or for the purpose of facilitating direct marketing by other organisations (APP 7.6). The organisation must give effect to any such request by an individual within a reasonable period of time and for free (APP 7.7). An organisation must, on request, notify an individual of its source of the individual's personal information that it has used or disclosed for the purpose of direct marketing unless this is unreasonable or impracticable to do so (APP 7.6).
17 When choices are provided to the individual offering the ability to limit the collection (question 14), use (question 15) and/or disclosure (question 16) of their personal information, are they displayed or provided in a clear and conspicuous manner?	Where the Applicant answers YES, the Accountability Agent must verify that the Applicant's choice mechanism is displayed in a clear and conspicuous manner. Where the Applicant answers NO, or when the Accountability Agent finds	APP 1, 2, 5, 6 & 7 APP1 APP 1.3 requires an APP entity to have a clearly expressed and up-to-date APP Privacy Policy about how it manages personal information. APP 1.4 contains a non-exhaustive list of information that an APP entity must include in its APP Privacy Policy:

	that the Applicant's choice mechanism is not displayed in a clear and conspicuous manner, the Accountability Agent must inform the Applicant that all mechanisms that allow individuals to exercise choice in relation to the collection, use, and/or disclosure of their personal information, must be clear and conspicuous in order to comply with this principle.	- the kinds of personal information collected and held by the entity (APP 1.4(a)) - how personal information is collected and held (APP 1.4(b)) - the purposes for which personal information is collected, held, used and disclosed (APP 1.4(c)) - how an individual may access their personal information and seek its correction (APP 1.4(d)) - how an individual may complain if the entity breaches the APPs or any registered binding APP code, and how the complaint will be handled (APP 1.4(e)) - whether the entity is likely to disclose personal information to overseas recipients (APP 1.4(f)), 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 (APP 1.4(g)). APP2 APP 2 provides that 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. That principle does not apply in relation to a particular matter if:

		- 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 (APP 2.2(a)), or - it is impracticable for the APP entity to deal with individuals who have not identified themselves or used a pseudonym (APP 2.2(b)). APP5 APP5 requires an APP entity that collects personal information about an individual to take reasonable steps either to notify the individual of certain matters or to ensure the individual is aware of those matters. Reasonable steps must be taken at or before the time of collection. The matters to be included in a notification include: - The APP entity's identity and contact details (APP 5.2(a)) - Facts and circumstances of collection (APP 5.2(b)) - If collection is required or authorised by law (APP 5.2(c)) - The purpose of collection (APP 5.2(d)) - Consequences for the individual if (APP 5.2(e)) personal information is not collected

		- Other APP entities, bodies or persons to which the personal information is usually disclosed (APP 5.2(f)) - Information about access and correction in the entity's Privacy Policy (APP 5.2(g)) - How the individual may complain about a breach of the APPs and how an entity will deal with such complaint (APP5.2(h)) - Likely cross-border disclosure of personal information (APP 5.2(i)) - When notification is to occur (APP 5.1) The requirement to notify applies to all personal information 'collected' about an individual, either directly from the individual or from a third party. APP 6 APP 6 outlines when an APP entity may use or disclose personal information. An APP entity can only use or disclose personal information for a purpose for which it was collected (known as the 'primary purpose'), or for a secondary purpose if an exception applies. The exceptions include where: - the individual has consented to a secondary use or disclosure (APP6.1(a)) - the individual would reasonably expect the APP entity to use or disclose their personal information

		for the secondary purpose, and that purpose is related to the primary purpose of collection, or, in the case of sensitive information, directly related to the primary purpose (APP6.2(a)). - the secondary use or disclosure is required or authorised by or under an Australian law or a court/tribunal order (APP6.2(b)) - a permitted general situation exists in relation to the secondary use or disclosure (APP6.2(c)) - the APP entity is an organisation and a permitted health situation exists in relation to the secondary use or disclosure (APP6.2(d)) - the APP entity reasonably believes that the secondary use or disclosure is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body,(APP6.2(e)) or - the APP entity is a government agency (other than an enforcement body) and discloses biometric information or biometric templates to an enforcement body, and the disclosure is conducted in accordance with guidelines made by the Information Commissioner for the purposes of APP 6.3 (APP6.3). An APP entity may disclose personal information,

		other than sensitive information, to a related body corporate (s 13B(1)(b)). APP 6 does not apply to the use or disclosure by an organisation of: - personal information for the purpose of direct marketing (this is covered by APP 7), or - government related identifiers (this is covered by APP 9) (APP 6.7). APP7 APP 7 provides that an organisation must not use or disclose personal information it holds for the purpose of direct marketing unless an exception applies (APP 7.1). The exceptions in APP 7.2 and 7.3 apply to personal information other than sensitive information. They draw a distinction between the use or disclosure of personal information by an organisation where: - the personal information has been collected directly from an individual, and the individual would reasonably expect their personal information to be used for the purpose of direct marketing (APP 7.2), and - the personal information has been collected from

		a third party, or from the individual directly but the individual does not have a reasonable expectation that their personal information will be used for the purpose of direct marketing (APP 7.3). Sources of third party data include data list providers, third party mobile applications, third party lead generation and enhancement data. Exceptions to this principle also apply in relation to: - sensitive information (APP 7.4), and - an organisation that is a contracted service provider for a Commonwealth contract (APP 7.5). An individual may request an organisation not to use or disclose their personal information for the purpose of direct marketing, or for the purpose of facilitating direct marketing by other organisations (APP 7.6). The organisation must give effect to any such request by an individual within a reasonable period of time and for free (APP 7.7). An organisation must, on request, notify an individual of its source of the individual's personal information that it has used or disclosed for the purpose of direct marketing unless this is unreasonable or impracticable to do so (APP 7.6).
18. When choices are provided to the individual offering the ability to limit	Where the Applicant answers YES, the Accountability Agent must verify that	APP 1, 2, 5, 6 & 7 APP1

the collection (question 14), use (question 15) and/or disclosure (question 16) of their personal information, are they clearly worded and easily understandable?	the Applicant's choice mechanism is clearly worded and easily understandable. Where the Applicant answers NO, and/or when the Accountability Agent finds that the Applicant's choice mechanism is not clearly worded and easily understandable, the Accountability Agent must inform the Applicant that all mechanisms that allow individuals to exercise choice in relation to the collection, use, and/or disclosure of their personal information, must be clearly worded and easily understandable in order to comply with this principle.	APP 1.3 requires an APP entity to have a clearly expressed and up-to-date APP Privacy Policy about how it manages personal information. APP 1.4 contains a non-exhaustive list of information that an APP entity must include in its APP Privacy Policy: - the kinds of personal information collected and held by the entity (APP 1.4(a)) - how personal information is collected and held (APP 1.4(b)) - the purposes for which personal information is collected, held, used and disclosed (APP 1.4(c)) - how an individual may access their personal information and seek its correction (APP 1.4(d)) - how an individual may complain if the entity breaches the APPs or any registered binding APP code, and how the complaint will be handled (APP 1.4(e)) - whether the entity is likely to disclose personal information to overseas recipients (APP 1.4(f)), 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 (APP 1.4(g)).

		APP2 APP 2 provides that 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. That principle does not apply in relation to a particular matter if: - 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 (APP 2.2(a)), or - it is impracticable for the APP entity to deal with individuals who have not identified themselves or used a pseudonym (APP 2.2(b)). APP5 APP5 requires an APP entity that collects personal information about an individual to take reasonable steps either to notify the individual of certain matters or to ensure the individual is aware of those matters. Reasonable steps must be taken at or before the time of collection. The matters to be included in a notification include: - The APP entity's identity and contact details (APP 5.2(a)) - Facts and circumstances of collection (APP

		5.2(b)) - If collection is required or authorised by law (APP 5.2(c)) - The purpose of collection (APP 5.2(d)) - Consequences for the individual if (APP 5.2(e)) personal information is not collected - Other APP entities, bodies or persons to which the personal information is usually disclosed (APP 5.2(f)) - Information about access and correction in the entity's Privacy Policy (APP 5.2(g)) - How the individual may complain about a breach of the APPs and how an entity will deal with such complaint (APP5.2(h)) - Likely cross-border disclosure of personal information (APP 5.2(i)) - When notification is to occur (APP 5.1) The requirement to notify applies to all personal information 'collected' about an individual, either directly from the individual or from a third party. APP6 APP 6 outlines when an APP entity may use or disclose personal information. An APP entity can only use or disclose personal information for a

		purpose for which it was collected (known as the 'primary purpose'), or for a secondary purpose if an exception applies. The exceptions include where: - the individual has consented to a secondary use or disclosure (APP6.1(a)) - the individual would reasonably expect the APP entity to use or disclose their personal information for the secondary purpose, and that purpose is related to the primary purpose of collection, or, in the case of sensitive information, directly related to the primary purpose (APP6.2(a)). - the secondary use or disclosure is required or authorised by or under an Australian law or a court/tribunal order (APP6.2(b)) - a permitted general situation exists in relation to the secondary use or disclosure (APP6.2(c)) - the APP entity is an organisation and a permitted health situation exists in relation to the secondary use or disclosure (APP6.2(d)) - the APP entity reasonably believes that the secondary use or disclosure is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body,(APP6.2(e)) or - the APP entity is a government agency (other than

		an enforcement body) and discloses biometric information or biometric templates to an enforcement body, and the disclosure is conducted in accordance with guidelines made by the Information Commissioner for the purposes of APP 6.3 (APP6.3). An APP entity may disclose personal information, other than sensitive information, to a related body corporate (s 13B(1)(b)). APP 6 does not apply to the use or disclosure by an organisation of: - personal information for the purpose of direct marketing (this is covered by APP 7), or - government related identifiers (this is covered by APP 9) (APP 6.7). APP7 APP 7 provides that an organisation must not use or disclose personal information it holds for the purpose of direct marketing unless an exception applies (APP 7.1). The exceptions in APP 7.2 and 7.3 apply to personal information other than sensitive information. They draw a distinction between the use or disclosure of

		personal information by an organisation where: - the personal information has been collected directly from an individual, and the individual would reasonably expect their personal information to be used for the purpose of direct marketing (APP 7.2), and - the personal information has been collected from a third party, or from the individual directly but the individual does not have a reasonable expectation that their personal information will be used for the purpose of direct marketing (APP 7.3). Sources of third party data include data list providers, third party mobile applications, third party lead generation and enhancement data. Exceptions to this principle also apply in relation to: - sensitive information (APP 7.4), and - an organisation that is a contracted service provider for a Commonwealth contract (APP 7.5). An individual may request an organisation not to use or disclose their personal information for the purpose of direct marketing, or for the purpose of facilitating direct marketing by other organisations (APP 7.6). The organisation must give effect to any such request by an individual within a reasonable period of time

		and for free (APP 7.7). An organisation must, on request, notify an individual of its source of the individual's personal information that it has used or disclosed for the purpose of direct marketing unless this is unreasonable or impracticable to do so (APP 7.6).
19. When choices are provided to the individual offering the ability to limit the collection (question 14), use (question 15) and/or disclosure (question 16) of their personal information, are these choices easily accessible and affordable? Where YES, describe.	Where the Applicant answers YES, the Accountability Agent must verify that the Applicant's choice mechanism is easily accessible and affordable. Where the Applicant answers NO, or when the Accountability Agent finds that the Applicant's choice mechanism is not easily accessible and affordable, the Accountability Agent must inform the Applicant that all mechanisms that allow individuals to exercise choice in relation to the collection, use, and/or disclosure of their personal information, must be easily accessible and affordable in order to comply with this principle.	APP 1, 5, 6 & 7 APP1 APP 1.3 requires an APP entity to have a clearly expressed and up-to-date APP Privacy Policy about how it manages personal information. APP 1.4 contains a non-exhaustive list of information that an APP entity must include in its APP Privacy Policy: - the kinds of personal information collected and held by the entity (APP 1.4(a)) - how personal information is collected and held (APP 1.4(b)) - the purposes for which personal information is collected, held, used and disclosed (APP 1.4(c)) - how an individual may access their personal information and seek its correction (APP 1.4(d)) - how an individual may complain if the entity breaches the APPs or any registered binding APP code, and how the complaint will be handled

		(APP 1.4(e)) - whether the entity is likely to disclose personal information to overseas recipients (APP 1.4(f)), 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 (APP 1.4(g)). - APP 1.5 requires and entity to take reasonable steps to make its APP Privacy Policy available free of charge in an appropriate form and, upon request, in a particular form (APP 1.6). APP5 APP 5requires an APP entity that collects personal information about an individual to take reasonable steps either to notify the individual of certain matters or to ensure the individual is aware of those matters. Reasonable steps must be taken at or before the time of collection, or as soon as practicable afterwards. The matters to be included in a notification include: - The APP entity's identity and contact details - Facts and circumstances of collection - If collection is required or authorised by law - The purpose of collection - Consequences for the individual if personal

		information is not collected - Other APP entities, bodies or persons to which the personal information is usually disclosed - Information about access and correction in the entity's Privacy Policy - Likely cross-border disclosure of personal information - When notification is to occur. The requirement to notify applies to all personal information 'collected' about an individual, either directly from the individual or from a third party. APP6 APP 6 outlines when an APP entity may use or disclose personal information. An APP entity can only use or disclose personal information for a purpose for which it was collected (known as the 'primary purpose'), or for a secondary purpose if an exception applies. The exceptions include where: - the individual has consented to a secondary use or disclosure (APP6.1(a)) - the individual would reasonably expect the APP entity to use or disclose their personal information for the secondary purpose, and that purpose is related to the primary purpose of collection, or, in

		the case of sensitive information, directly related to the primary purpose (APP6.2(a)). - the secondary use or disclosure is required or authorised by or under an Australian law or a court/tribunal order (APP6.2(b)) - a permitted general situation exists in relation to the secondary use or disclosure (APP6.2(c)) - the APP entity is an organisation and a permitted health situation exists in relation to the secondary use or disclosure (APP6.2(d)) - the APP entity reasonably believes that the secondary use or disclosure is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body,(APP6.2(e)) or - the APP entity is a government agency (other than an enforcement body) and discloses biometric information or biometric templates to an enforcement body, and the disclosure is conducted in accordance with guidelines made by the Information Commissioner for the purposes of APP 6.3 (APP6.3). An APP entity may disclose personal information, other than sensitive information, to a related body corporate (s 13B(1)(b)).

		APP 6 does not apply to the use or disclosure by an organisation of: - personal information for the purpose of direct marketing (this is covered by APP 7), or - government related identifiers (this is covered by APP 9) (APP 6.7). APP7 APP 7 provides that an organisation must not use or disclose personal information it holds for the purpose of direct marketing unless an exception applies (APP 7.1). The exceptions in APP 7.2 and 7.3 apply to personal information other than sensitive information. They draw a distinction between the use or disclosure of personal information by an organisation where: - the personal information has been collected directly from an individual, and the individual would reasonably expect their personal information to be used for the purpose of direct marketing (APP 7.2), and - the personal information has been collected from a third party, or from the individual directly but the individual does not have a reasonable

		expectation that their personal information will be used for the purpose of direct marketing (APP 7.3). Sources of third party data include data list providers, third party mobile applications, third party lead generation and enhancement data. Exceptions to this principle also apply in relation to: - sensitive information (APP 7.4), and - an organisation that is a contracted service provider for a Commonwealth contract (APP 7.5). An individual may request an organisation not to use or disclose their personal information for the purpose of direct marketing, or for the purpose of facilitating direct marketing by other organisations (APP 7.6). The organisation must give effect to any such request by an individual within a reasonable period of time and for free (APP 7.7). An organisation must, on request, notify an individual of its source of the individual's personal information that it has used or disclosed for the purpose of direct marketing unless this is unreasonable or impracticable to do so (APP 7.6).
20. What mechanisms are in place so that choices, where appropriate, can be honored in an effective and expeditious	Where the Applicant does have mechanisms in place, the Accountability Agent must require the Applicant to	APP 1, 5, 6 & 7 APP1 APP 1.3 requires an APP entity to have a clearly

manner? Provide a description in the space below or in an attachment if necessary. Describe below.	provide of the relevant policy or procedures specifying how the preferences expressed through the choice mechanisms (questions 14, 15 and 16) are honored. Where the Applicant does not have mechanisms in place, the Applicant must identify the applicable qualification to the provision of choice and provide a description and the Accountability Agent must verify whether the applicable qualification is justified. Where the Applicant answers NO and does not provide an acceptable qualification, the Accountability Agent must inform the Applicant that a mechanism to ensure that choices, when offered, can be honored, must be provided.	expressed and up-to-date APP Privacy Policy about how it manages personal information. APP 1.4 contains a non-exhaustive list of information that an APP entity must include in its APP Privacy Policy: - the kinds of personal information collected and held by the entity (APP 1.4(a)) - how personal information is collected and held (APP 1.4(b)) - the purposes for which personal information is collected, held, used and disclosed (APP 1.4(c)) - how an individual may access their personal information and seek its correction (APP 1.4(d)) - how an individual may complain if the entity breaches the APPs or any registered binding APP code, and how the complaint will be handled (APP 1.4(e)) - whether the entity is likely to disclose personal information to overseas recipients (APP 1.4(f)), 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 (APP 1.4(g)). APP 1.5 requires and entity to take reasonable steps to make its APP Privacy Policy available free of

		charge in an appropriate form and, upon request, in a particular form (APP 1.6). APP5 - APP 5 requires an APP entity that collects personal information about an individual to take reasonable steps either to notify the individual of certain matters or to ensure the individual is aware of those matters. Reasonable steps must be taken at or before the time of collection, or as soon as practicable afterwards. The matters to be included in a notification include: - The APP entity's identity and contact details - Facts and circumstances of collection - If collection is required or authorised by law - The purpose of collection - Consequences for the individual if personal information is not collected - Other APP entities, bodies or persons to which the personal information is usually disclosed - Information about access and correction in the entity's Privacy Policy - Likely cross-border disclosure of personal information

		- When notification is to occur. The requirement to notify applies to all personal information 'collected' about an individual, either directly from the individual or from a third party. APP6 APP 6 outlines when an APP entity may use or disclose personal information. An APP entity can only use or disclose personal information for a purpose for which it was collected (known as the 'primary purpose'), or for a secondary purpose if an exception applies. The exceptions include where: - the individual has consented to a secondary use or disclosure (APP6.1(a)) - the individual would reasonably expect the APP entity to use or disclose their personal information for the secondary purpose, and that purpose is related to the primary purpose of collection, or, in the case of sensitive information, directly related to the primary purpose (APP6.2(a)). - the secondary use or disclosure is required or authorised by or under an Australian law or a court/tribunal order (APP6.2(b)) - a permitted general situation exists in relation to the secondary use or disclosure (APP6.2(c)) - the APP entity is an organisation and a permitted

		health situation exists in relation to the secondary use or disclosure (APP6.2(d)) - the APP entity reasonably believes that the secondary use or disclosure is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body,(APP6.2(e)) or - the APP entity is a government agency (other than an enforcement body) and discloses biometric information or biometric templates to an enforcement body, and the disclosure is conducted in accordance with guidelines made by the Information Commissioner for the purposes of APP 6.3 (APP6.3). An APP entity may disclose personal information, other than sensitive information, to a related body corporate (s 13B(1)(b)). APP 6 does not apply to the use or disclosure by an organisation of: - personal information for the purpose of direct marketing (this is covered by APP 7), or - government related identifiers (this is covered by APP 9) (APP 6.7). APP7 APP 7 provides that an organisation must not use or

		disclose personal information it holds for the purpose of direct marketing unless an exception applies (APP 7.1). The exceptions in APP 7.2 and 7.3 apply to personal information other than sensitive information. They draw a distinction between the use or disclosure of personal information by an organisation where: - the personal information has been collected directly from an individual, and the individual would reasonably expect their personal information to be used for the purpose of direct marketing (APP 7.2), and - the personal information has been collected from a third party, or from the individual directly but the individual does not have a reasonable expectation that their personal information will be used for the purpose of direct marketing (APP 7.3). Sources of third party data include data list providers, third party mobile applications, third party lead generation and enhancement data. Exceptions to this principle also apply in relation to: - sensitive information (APP 7.4), and - an organisation that is a contracted service provider for a Commonwealth contract (APP 7.5).

		An individual may request an organisation not to use or disclose their personal information for the purpose of direct marketing, or for the purpose of facilitating direct marketing by other organisations (APP 7.6). The organisation must give effect to any such request by an individual within a reasonable period of time and for free (APP 7.7). An organisation must, on request, notify an individual of its source of the individual's personal information that it has used or disclosed for the purpose of direct marketing unless this is unreasonable or impracticable to do so (APP 7.6).

INTEGRITY OF PERSONAL INFORMATION

Assessment Purpose - *The questions in this section are directed towards ensuring that the personal information controller maintains the accuracy and completeness of records and keeps them up to date. This Principle also recognizes that these obligations are only required to the extent necessary for the purposes of use*

Question (*to be answered by the Applicant*)	Assessment Criteria (*to be verified by the Accountability Agent*)	Enforceability (*to be answered by the Economy*)
21. Do you take steps to verify that the personal information held by you is up to date, accurate and complete, to the extent necessary for the purposes of use?	Where the Applicant answers YES, the Accountability Agent must require the Applicant to provide the procedures the Applicant has in place to verify and	The alignment of CBPR requirements for ensuring the integrity of personal information under this heading may require further consideration during development of the proposed code (pursuant to Part

If YES, describe.	ensure that the personal information held is up to date, accurate and complete, to the extent necessary for the purposes of use. The Accountability Agent will verify that reasonable procedures are in place to allow the Applicant to maintain personal information that is up to date, accurate and complete, to the extent necessary for the purpose of use. Where the Applicant answers NO, the Accountability Agent must inform the Applicant that procedures to verify and ensure that the personal information held is up to date, accurate and complete, to the extent necessary for the purposes of use, are required for compliance with this principle.	IIIB of the Privacy Act). For example, where CBPR program requirements require corrections made to personal information to be communicated to third parties, the APPs only require this to be done when directly requested by an individual. APP 10, 11, 13 APP 10 APP 10 provides that an APP entity must take reasonable steps to ensure the quality of personal information it collects, uses or discloses (APP 10)). If reasonable steps are taken to comply with APP 10, this reduces the likelihood that personal information will need correction (under APP 13) APP 11 APP entity must take reasonable steps to protect the personal information it holds, including from interference, loss and unauthorised modification (APP 11.1). If reasonable steps are taken to comply with APP 11.1, this reduces the likelihood that personal information will need correction (under APP 13). APP 13 APP 13 relates to correction of personal information. It operates alongside and does not replace other informal or legal procedures by which an individual

		can seek correction of their personal information, including informal arrangements and, for government agencies, the *Freedom of Information Act 1982* (FOI Act). APP 13.1 provides that an APP entity must take reasonable steps to correct personal information it holds, to ensure it is accurate, up-to-date, complete, relevant and not misleading, having regard to the purpose for which it is held. The requirement to take reasonable steps applies in two circumstances: - where an APP entity is satisfied, independently of any request, that personal information it holds is incorrect, or - where an individual requests an APP entity to correct their personal information. Special considerations apply to Commonwealth records. A Commonwealth record can, as a general rule, only be destroyed or altered in accordance with the Archives Act (see paragraph 13.48). APP 13 also sets out other minimum procedural requirements in relation to correcting personal information. An APP entity must:

		- upon request by an individual whose personal information has been corrected, take reasonable steps to notify another APP entity of a correction made to personal information that was previously provided to that other entity (APP 13.2) - give a written notice to an individual when a correction request is refused, including the reasons for the refusal and the complaint mechanisms available to the individual (APP 13.3) - upon request by an individual whose correction request has been refused, take reasonable steps to associate a statement with the personal information that the individual believes it to be incorrect. - respond in a timely manner to an individual's request to correct personal information or to associate a statement with the personal information (APP 13.5(a)) - not charge an individual for making a request to correct personal information or associate a statement, or for making a correction or associating a statement (APP 13.5(b)). When taking steps to identify and correct incorrect personal information under APP 13, an entity should

		consider whether it still needs the personal information for a permitted purpose, or whether reasonable steps must be taken to destroy or de-identify the information (under APP 11.2).
22. Do you have a mechanism for correcting inaccurate, incomplete and out-dated personal information to the extent necessary for purposes of use? Provide a description	Where the Applicant answers YES, the Accountability Agent must require the Applicant to provide the procedures and steps the Applicant has in place for correcting inaccurate, incomplete and out-dated personal information, which includes, but is not limited to, procedures which allows individuals to challenge the accuracy of information such as accepting a request for correction from individuals by e-mail, post, phone or fax, through a website, or by some other method. The Accountability Agent must verify that this process is in place and operational. Where the Applicant answers NO, the Accountability Agent must inform the Applicant that procedures/steps to verify and ensure that the personal information held is up to date, accurate and complete, to the extent necessary for the purposes of use, are required for compliance with this principle.	APP 1, 10, 11 APP 1 APP 1.4 contains a non-exhaustive list of information that an APP entity must include in its APP Privacy Policy: - the kinds of personal information collected and held by the entity (APP 1.4(a)) - how personal information is collected and held (APP 1.4(b)) - the purposes for which personal information is collected, held, used and disclosed (APP 1.4(c)) - how an individual may access their personal information and seek its correction (APP 1.4(d)) - how an individual may complain if the entity breaches the APPs or any registered binding APP code, and how the complaint will be handled (APP 1.4(e)) - whether the entity is likely to disclose personal information to overseas recipients (APP 1.4(f)), 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 (APP 1.4(g)). APP 10 APP 10 provides that an APP entity must take reasonable steps to ensure the quality of personal information it collects, uses or discloses (APP 10). If reasonable steps are taken to comply with APP 10, this reduces the likelihood that personal information will need correction (under APP 13) APP 11 An APP entity must take reasonable steps to protect the personal information it holds, including from interference, loss and unauthorised modification (APP 11.1). If reasonable steps are taken to comply with APP 11.1, this reduces the likelihood that personal information will need correction (under APP 13).
23. Where inaccurate, incomplete or out of date information will affect the purposes of use and corrections are made to the information subsequent to the transfer of the information, do you communicate the corrections to personal information processors, agents, or other service providers to whom the personal	Where the Applicant answers YES, the Accountability Agent must require the Applicant to provide the procedures the Applicant has in place to communicate corrections to personal information processors, agent, or other service providers to whom the personal information was transferred and the	APP 13 An APP entity must, upon request by an individual whose personal information has been corrected, take reasonable steps to notify another APP entity of a correction made to personal information that was previously provided to that other entity (APP 13.2). (This requirement to communicate corrections to

information was transferred? If YES, describe.	accompanying procedures to ensure that the corrections are also made by the processors, agents or other service providers acting on the Applicant's behalf. The Accountability Agent must verify that these procedures are in place and operational, and that they effectively ensure that corrections are made by the processors, agents or other service providers acting on the Applicant's behalf. Where the Applicant answers NO, the Accountability Agent must inform the Applicant that procedures to communicate corrections to personal information processors, agent, or other service providers to whom the personal information was transferred, are required for compliance with this principle.	other providers only requires notification if requested by the individual).
24. Where inaccurate, incomplete or out of date information will affect the purposes of use and corrections are made to the information subsequent to the disclosure of the information, do you communicate the corrections to other third parties to whom the personal information was disclosed? If YES,	Where the Applicant answers YES, the Accountability Agent must require the Applicant to provide the procedures the Applicant has in place to communicate corrections to other third parties, to whom personal information was disclosed. The Accountability Agent must verify	APP 13 An APP entity must, upon request by an individual whose personal information has been corrected, take reasonable steps to notify another APP entity of a correction made to personal information that was previously provided to that other entity (APP 13.2). (This requirement to communicate corrections to

describe.	that these procedures are in place and operational. Where the Applicant answers NO, the Accountability Agent must inform the Applicant that procedures to communicate corrections to other third parties to whom personal information was disclosed, are required for compliance with this principle.	other providers only requires notification if requested by the individual).
25. Do you require personal information processors, agents, or other service providers acting on your behalf to inform you when they become aware of information that is inaccurate, incomplete, or out-of-date?	Where the Applicant answers YES, the Accountability Agent must require the Applicant to provide the procedures the Applicant has in place to receive corrections from personal information processors, agents, or other service providers to whom personal information was transferred or disclosed to ensure that personal information processors, agents, or other service providers to whom personal information was transferred inform the Applicant about any personal information known to be inaccurate incomplete, or outdated. The Accountability Agent will ensure that the procedures are in place and operational, and, where appropriate, lead to corrections being made by the	APP 10 APP 10 provides that an APP entity must take reasonable steps to ensure the quality of personal information it collects, uses or discloses (APP 10)). If reasonable steps are taken to comply with APP 10, this reduces the likelihood that personal information will need correction (under APP 13) APP 11 APP entity must take reasonable steps to protect the personal information it holds, including from interference, loss and unauthorised modification (APP 11.1). If reasonable steps are taken to comply with APP 11.1, this reduces the likelihood that personal information will need correction (under APP 13).

	Applicant and by the processors, agents or other service providers. Where the Applicant answers NO, the Accountability Agent must inform the Applicant that procedures to receive corrections from personal information processors, agents, or other service providers to whom personal information was transferred or disclosed, are required for compliance with this principle.	APP 13 APP 13 relates to correction of personal information. It operates alongside and does not replace other informal or legal procedures by which an individual can seek correction of their personal information, including informal arrangements and, for government agencies, the *Freedom of Information Act 1982* (FOI Act). APP 13.1 provides that an APP entity must take reasonable steps to correct personal information it holds, to ensure it is accurate, up-to-date, complete, relevant and not misleading, having regard to the purpose for which it is held. The requirement to take reasonable steps applies in two circumstances: - where an APP entity is satisfied, independently of any request, that personal information it holds is incorrect, or - where an individual requests an APP entity to correct their personal information. Special considerations apply to Commonwealth records. A Commonwealth record can, as a general rule, only be destroyed or altered in accordance with the Archives Act (see paragraph 13.48).

		APP 13 also sets out other minimum procedural requirements in relation to correcting personal information. An APP entity must: - upon request by an individual whose personal information has been corrected, take reasonable steps to notify another APP entity of a correction made to personal information that was previously provided to that other entity (APP 13.2) - give a written notice to an individual when a correction request is refused, including the reasons for the refusal and the complaint mechanisms available to the individual (APP 13.3) - upon request by an individual whose correction request has been refused, take reasonable steps to associate a statement with the personal information that the individual believes it to be incorrect. - respond in a timely manner to an individual's request to correct personal information or to associate a statement with the personal information (APP 13.5(a)) - not charge an individual for making a request to correct personal information or associate a statement, or for making a correction or

		associating a statement (APP 13.5(b)). When taking steps to identify and correct incorrect personal information under APP 13, an entity should consider whether it still needs the personal information for a permitted purpose, or whether reasonable steps must be taken to destroy or de-identify the information (under APP 11.2).

SECURITY SAFEGUARDS

Assessment Purpose - *The questions in this section are directed towards ensuring that when individuals entrust their information to an applicant, that applicant will implement reasonable security safeguards to protect individuals' information from loss, unauthorized access or disclosure, or other misuses*

Question (*to be answered by the Applicant*)	Assessment Criteria (*to be verified by the Accountability Agent*)	Enforceability (*to be answered by the Economy*)
26. Have you implemented an information security policy?	Where the Applicant answers YES, the Accountability Agent must verify the existence of this written policy. Where the Applicant answers NO, the Accountability Agent must inform the Applicant that the implementation of a written information security policy is required for compliance with this principle.	While the *Privacy Act 1988 1988* does not impose the specific information security requirements as stipulated under Q26, Q28 and Q29, they are envisaged as part of the broader security requirements in the Act. **Notifiable Data Breach Scheme** Under Part IIIC of the Privacy Act, the notifiable data breach scheme (NDB scheme) requires an APP entity to notify individuals and the Australian Information Commissioner where there has been an unauthorised access, disclosure or loss of personal information that a reasonable person would conclude is likely to result in serious harm to an individual (some limited exceptions apply). The Information Commissioner administers the NDB scheme and has powers to investigate and regulate non-

		compliance. APP 1, 8, 11 APP 1 APP 1.3 requires an APP entity to have a clearly expressed and up-to-date APP Privacy Policy about how it manages personal information. APP 1.4 contains a non-exhaustive list of information that an APP entity must include in its APP Privacy Policy: - the kinds of personal information collected and held by the entity (APP 1.4(a)) - how personal information is collected and held (APP 1.4(b)) - the purposes for which personal information is collected, held, used and disclosed (APP 1.4(c)) - how an individual may access their personal information and seek its correction (APP 1.4(d)) - how an individual may complain if the entity breaches the APPs or any registered binding APP code, and how the complaint will be handled (APP

		1.4(e)) - whether the entity is likely to disclose personal information to overseas recipients (APP 1.4(f)), 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 (APP 1.4(g)). APP 1.5 requires and entity to take reasonable steps to make its APP Privacy Policy available free of charge in an appropriate form and, upon request, in a particular form (APP 1.6). APP 8 APP 8 and s 16C of the *Privacy Act 1988 1988* create a framework for the cross-border disclosure of personal information. The framework generally requires an APP entity to ensure that an overseas recipient will handle an individual's personal information in accordance with the APPs, and makes the APP entity accountable if the overseas recipient mishandles the information. This reflects a central object of the

		Privacy Act of facilitating the free flow of information across national borders while ensuring that the privacy of individuals is respected (s 2A(f)). APP 8.1 provides that before an APP entity discloses personal information about an individual to an overseas recipient, the entity must take reasonable steps to ensure that the recipient does not breach the APPs in relation to that information. Where an entity discloses personal information to an overseas recipient, it is accountable for an act or practice of the overseas recipient that would breach the APPs (s 16C). The exceptions to the requirement in APP 8.1 and to the accountability provision in s 16C are: - Disclosing personal information to an overseas recipient that is subject to a substantially similar law or binding scheme and a readily accessible dispute resolution scheme (APP 8.2(a)) - Disclosing personal information to an overseas recipient with the individual's consent after the

		individual is expressly informed (APP 8.2(b)) - Disclosing personal information to an overseas recipient as required or authorised by law (APP 8.2(c)) - Disclosing personal information to an overseas recipient where a permitted particular situation exists (8.2(d)) - Disclosing personal information to an overseas recipient as required or authorised under an international agreement relating to information sharing (APP 8.2(e)) - Disclosing personal information to an overseas recipient for an enforcement related activity (APP 8.2(f)). When an APP entity discloses personal information to an overseas recipient it will also need to comply with APP 6. That is, it must only disclose the personal information for the primary purpose for which it was collected unless an exception to that principle applies. APP 11

		An APP entity must take reasonable steps to protect the personal information it holds, including from interference, loss and unauthorised modification (APP 11.1). If reasonable steps are taken to comply with APP 11.1, this reduces the likelihood that personal information will need correction (under APP 13).
27. Describe the physical, technical and administrative safeguards you have implemented to protect personal information against risks such as loss or unauthorized access, destruction, use, modification or disclosure of information or other misuses?	Where the Applicant provides a description of the physical, technical and administrative safeguards used to protect personal information, the Accountability Agent must verify the existence of such safeguards, which may include: □ Authentication and access control (eg password protections) □ Encryption □ Boundary protection (eg firewalls, intrusion detection) □ Audit logging □ Monitoring (eg external and internal audits, vulnerability scans) □ Other (specify) The Applicant must implement reasonable administrative, technical and physical safeguards, suitable to the	APP 1 APP 1.3 requires an APP entity to have a clearly expressed and up-to-date APP Privacy Policy about how it manages personal information. APP 1.4 contains a non-exhaustive list of information that an APP entity must include in its APP Privacy Policy: - the kinds of personal information collected and held by the entity (APP 1.4(a)) - how personal information is collected and held (APP 1.4(b)) - the purposes for which personal information is collected, held, used and disclosed (APP 1.4(c)) - how an individual may access their

	Applicant's size and complexity, the nature and scope of its activities, and the sensitivity of the personal information and/or Third Party personal information it collects, in order to protect that information from leakage, loss or unauthorized use, alteration, disclosure, distribution, or access. Such safeguards must be proportional to the probability and severity of the harm threatened the sensitivity of the information, and the context in which it is held. The Applicant must take reasonable measures to require information processors, agents, contractors, or other service providers to whom personal information is transferred to protect against leakage, loss or unauthorized access, destruction, use, modification or disclosure or other misuses of the information. The Applicant must periodically review and reassess its security measures to evaluate their relevance and effectiveness. Where the Applicant indicates that it has NO physical, technical and administrative safeguards, or inadequate safeguards, to	personal information and seek its correction (APP 1.4(d)) - how an individual may complain if the entity breaches the APPs or any registered binding APP code, and how the complaint will be handled (APP 1.4(e)) - whether the entity is likely to disclose personal information to overseas recipients (APP 1.4(f)), 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 (APP 1.4(g)). APP 1.5 requires and entity to take reasonable steps to make its APP Privacy Policy available free of charge in an appropriate form and, upon request, in a particular form (APP 1.6). APP 8 APP 8 and s 16C of the *Privacy Act 1988 1988* create a framework for the cross-border disclosure of personal information. The framework generally requires an APP entity to ensure that an

	protect personal information, the Accountability Agent must inform the Applicant that the implementation of such safeguards is required for compliance with this principle.	overseas recipient will handle an individual's personal information in accordance with the APPs, and makes the APP entity accountable if the overseas recipient mishandles the information. This reflects a central object of the Privacy Act 1988, of facilitating the free flow of information across national borders while ensuring that the privacy of individuals is respected (s 2A(f)). APP 8.1 provides that before an APP entity discloses personal information about an individual to an overseas recipient, the entity must take reasonable steps to ensure that the recipient does not breach the APPs in relation to that information. Where an entity discloses personal information to an overseas recipient, it is accountable for an act or practice of the overseas recipient that would breach the APPs (s 16C). The exceptions to the requirement in APP 8.1 and to the accountability provision in s 16C are: - Disclosing personal information to an overseas recipient that is subject to a substantially similar law or binding

		scheme and a readily accessible dispute resolution scheme (APP 8.2(a)) - Disclosing personal information to an overseas recipient with the individual's consent after the individual is expressly informed (APP 8.2(b)) - Disclosing personal information to an overseas recipient as required or authorised by law (APP 8.2(c)) - Disclosing personal information to an overseas recipient where a permitted particular situation exists (8.2(d)) - Disclosing personal information to an overseas recipient as required or authorised under an international agreement relating to information sharing (APP 8.2(e)) - Disclosing personal information to an overseas recipient for an enforcement related activity (APP 8.2(f)). When an APP entity discloses personal information to an overseas recipient it will also need to comply with APP 6.

		That is, it must only disclose the personal information for the primary purpose for which it was collected unless an exception to that principle applies. APP 11 An APP entity must take reasonable steps to protect the personal information it holds, including from interference, loss and unauthorised modification (APP 11.1). If reasonable steps are taken to comply with APP 11.1, this reduces the likelihood that personal information will need correction (under APP 13). **Notifiable Data Breach Scheme** Under Part IIIC of the Privacy Act, the notifiable data breach scheme (NDB scheme) requires an APP entity to notify individuals and the Australian Information Commissioner where there has been an unauthorised access, disclosure or loss of personal information that a reasonable person would conclude is likely to result in serious harm to an individual (some limited exceptions apply). The Information Commissioner administers the NDB scheme and has

		powers to investigate and regulate non-compliance.
28. Describe how the safeguards you identified in response to question 27 are proportional to the likelihood and severity of the harm threatened, the sensitivity of the information, and the context in which it is held.	Where the Applicant provides a description of the physical, technical and administrative safeguards used to protect personal information, the Accountability Agent must verify that these safeguards are proportional to the risks identified. The Applicant must implement reasonable administrative, technical and physical safeguards, suitable to the Applicant's size and complexity, the nature and scope of its activities, and the confidentiality or sensitivity of the personal information (whether collected directly from the individuals or through a third party) it gathers, in order to protect that information from unauthorized leakage, loss, use, alteration, disclosure, distribution, or access.	APP 11 An APP entity must take reasonable steps to protect the personal information it holds, including from interference, loss and unauthorised modification (APP 11.1).
29. Describe how you make your employees aware of the importance of maintaining the security of personal information (e.g. through regular training and oversight).	The Accountability Agent must verify that the Applicant's employees are aware of the importance of, and obligations respecting, maintaining the security of personal information through regular training and oversight as demonstrated by	APP 11 An APP entity must take reasonable steps to protect the personal information it holds, including from interference, loss and unauthorised modification (APP 11.1). If reasonable steps are taken to

	procedures, which may include: □ Training program for employees □ Regular staff meetings or other communications □ Security policy signed by employees □ Other (specify) Where the Applicant answers that it does not make employees aware of the importance of, and obligations respecting, maintaining the security of personal information through regular training and oversight, the Accountability Agent has to inform the Applicant that the existence of such procedures are required for compliance with this principle.	comply with APP 11.1, this reduces the likelihood that personal information will need correction (under APP 13). Relevant guidelines (that are not legally binding) issued by the Office of the Australian Information Commissioner) stipulate that entities bound by the Privacy Act should consider whether they have documented policies that address security matters, such as physical, ICT, security and other appropriate information handling practices (OAIC's Guide to securing personal information).
30. Have you implemented safeguards that are proportional to the likelihood and severity of the harm threatened, the sensitivity of the information, and the context in which it is held through: 30.a) Employee training and management or other safeguards? 30.b) Information systems and management, including network and software design, as well as information processing, storage, transmission, and	Where the Applicant answers YES (to questions 30.a to 30.d), the Accountability Agent has to verify the existence each of the safeguards. The safeguards have to be proportional to the probability and severity of the harm threatened, the confidential nature or sensitivity of the information, and the context in which it is held. The Applicant must employ suitable and reasonable means, such as encryption, to protect all	APP 11 An APP entity must take reasonable steps to protect the personal information it holds, including from interference, loss and unauthorised modification (APP 11.1). If reasonable steps are taken to comply with APP 11.1, this reduces the likelihood that personal information will need correction (under APP 13). Relevant guidelines (that are not legally

disposal? 30.c) Detecting, preventing, and responding to attacks, intrusions, or other security failures? 30.d) Physical security?	personal information. Where the Applicant answers NO (to questions 30.a to 30.d), the Accountability Agent must inform the Applicant that the existence of safeguards on each category is required for compliance with this principle.	binding) issued by the Office of the Australian Information Commissioner) stipulate that entities bound by the Privacy Act should consider whether they have documented policies that address security matters, such as physical, ICT, security and other appropriate information handling practices (OAIC's Guide to securing personal information). **Notifiable Data Breach Scheme** Under Part IIIC of the Privacy Act, the notifiable data breach scheme (NDB scheme) requires an APP entity to notify individuals and the Australian Information Commissioner where there has been an unauthorised access, disclosure or loss of personal information that a reasonable person would conclude is likely to result in serious harm to an individual (some limited exceptions apply). The Information Commissioner administers the NDB scheme and has powers to investigate and regulate non-compliance.
31. Have you implemented a policy for secure disposal of personal information?	Where the Applicant answers YES, the Accountability Agent must verify the implementation of a policy for the secure	APP 11 An APP entity must take reasonable steps to protect the personal information it

	disposal of personal information. Where the Applicant answers NO, the Accountability Agent must inform Applicant that the existence of a policy for the secure disposal of personal information is required for compliance with this principle.	holds, including from interference, loss and unauthorised modification (APP 11.1). If reasonable steps are taken to comply with APP 11.1, this reduces the likelihood that personal information will need correction (under APP 13). An APP entity must take reasonable steps to destroy or de-identify the personal information it holds once the personal information is no longer needed for any purpose for which the personal information may be used or disclosed under the APPs. This requirement does not apply where the personal information is contained in a Commonwealth record or where the entity is required by law or a court/tribunal order to retain the personal information (APP 11.2).
32. Have you implemented measures to detect, prevent, and respond to attacks, intrusions, or other security failures?	Where the Applicant answers YES, the Accountability Agent must verify the existence of measures to detect, prevent, and respond to attacks, intrusions, or other security failures. Where the Applicant answers NO, the Accountability Agent must inform the Applicant that the existence of measures	APP 11 An APP entity must take reasonable steps to protect the personal information it holds, including from interference, loss and unauthorised modification (APP 11.1). If reasonable steps are taken to comply with APP 11.1, this reduces the likelihood that personal information will

	to detect, prevent, and respond to attacks, intrusions, or other security failures, is required for compliance with this principle.	need correction (under APP 13). Relevant guidelines (that are not legally binding) issued by the Office of the Australian Information Commissioner stipulate that entities bound by the Privacy Act should consider whether they have documented policies that address security matters, such as physical, ICT, security and other appropriate information handling practices (OAIC's Guide to securing personal information). **Notifiable Data Breach Scheme** Under Part IIIC of the Privacy Act, the notifiable data breach scheme (NDB scheme) requires an APP entity to notify individuals and the Australian Information Commissioner where there has been an unauthorised access, disclosure or loss of personal information that a reasonable person would conclude is likely to result in serious harm to an individual (some limited exceptions apply). The Information Commissioner administers the NDB scheme and has powers to investigate and regulate non-compliance.

33. Do you have processes in place to test the effectiveness of the safeguards referred to above in question 32? Describe below.	The Accountability Agent must verify that such tests are undertaken at appropriate intervals, and that the Applicant adjusts their security safeguards to reflect the results of these tests.	APP 11 An APP entity must take reasonable steps to protect the personal information it holds, including from interference, loss and unauthorised modification (APP 11.1). If reasonable steps are taken to comply with APP 11.1, this reduces the likelihood that personal information will need correction (under APP 13). Relevant guidelines (that are not legally binding) issued by the Office of the Australian Information Commissioner stipulate that entities bound by the Privacy Act should consider whether they have documented policies that address security matters, such as physical, ICT, security and other appropriate information handling practices (OAIC's Guide to securing personal information).
34. Do you use risk assessments or third-party certifications? Describe below.	The Accountability Agent must verify that such risk assessments or certifications are undertaken at appropriate intervals, and that the Applicant adjusts their security safeguards to reflect the results of these certifications or risk assessments. One example is whether privacy compliance	APP 11 An APP entity must take reasonable steps to protect the personal information it holds, including from interference, loss and unauthorised modification (APP 11.1). If reasonable steps are taken to comply with APP 11.1, this reduces the likelihood that personal information will

	audits are carried out by the Applicant and if audits are carried out, the Accountability Agent must verify whether recommendations made in the audits are implemented.	need correction (under APP 13). Relevant guidelines (that are not legally binding) issued by the Office of the Australian Information Commissioner stipulate that entities bound by the Privacy Act should consider whether they have documented policies that address security matters, such as physical, ICT, security and other appropriate information handling practices (OAIC's Guide to securing personal information).
35. Do you require personal information processors, agents, contractors, or other service providers to whom you transfer personal information to protect against loss, or unauthorized access, destruction, use, modification or disclosure or other misuses of the information by: 35.a) Implementing an information security program that is proportionate to the sensitivity of the information and services provided? 35.b) Notifying you promptly when they become aware of an occurrence of breach of the privacy or security of the personal information of the Applicant's customers?	The Accountability Agent must verify that the Applicant has taken reasonable measures (such as by inclusion of appropriate contractual provisions) to require information processors, agents, contractors, or other service providers to whom personal information is transferred, to protect against leakage, loss or unauthorized access, destruction, use, modification or disclosure or other misuses of the information. The Applicant must periodically review and reassess its security measures to evaluate their relevance and effectiveness.	APP 8, 11, Notifiable Data Breach Scheme (Part IIIC Privacy Act) APP8 APP 8 and s 16C of the Privacy Act create a framework for the cross-border disclosure of personal information. The framework generally requires an APP entity to ensure that an overseas recipient will handle an individual's personal information in accordance with the APPs, and makes the APP entity accountable if the overseas recipient mishandles the information. This reflects a central object of the Privacy Act 1988, of facilitating the free

35.c) Taking immediate steps to correct/address the security failure which caused the privacy or security breach?		flow of information across national borders while ensuring that the privacy of individuals is respected (s 2A(f)). APP 8.1 provides that before an APP entity discloses personal information about an individual to an overseas recipient, the entity must take reasonable steps to ensure that the recipient does not breach the APPs in relation to that information. Where an entity discloses personal information to an overseas recipient, it is accountable for an act or practice of the overseas recipient that would breach the APPs (s 16C). The exceptions to the requirement in APP 8.1 and to the accountability provision in s 16C are: - Disclosing personal information to an overseas recipient that is subject to a substantially similar law or binding scheme and a readily accessible dispute resolution scheme (APP 8.2(a)) - Disclosing personal information to an overseas recipient with the individual's consent after the individual is expressly informed (APP

		8.2(b)) - Disclosing personal information to an overseas recipient as required or authorised by law (APP 8.2(c)) - Disclosing personal information to an overseas recipient where a permitted particular situation exists (8.2(d)) - Disclosing personal information to an overseas recipient as required or authorised under an international agreement relating to information sharing (APP 8.2(e)) - Disclosing personal information to an overseas recipient for an enforcement related activity (APP 8.2(f)) When an APP entity discloses personal information to an overseas recipient it will also need to comply with APP 6. That is, it must only disclose the personal information for the primary purpose for which it was collected unless an exception to that principle applies. APP 11 An APP entity must take reasonable steps

		to protect the personal information it holds, including from interference, loss and unauthorised modification (APP 11.1). If reasonable steps are taken to comply with APP 11.1, this reduces the likelihood that personal information will need correction (under APP 13). Relevant guidelines (that are not legally binding) issued by the Office of the Australian Information Commissioner) stipulate that entities bound by the Privacy Act should consider whether they have documented policies that address security matters, such as physical, ICT, security and other appropriate information handling practices (OAIC's Guide to securing personal information). **Notifiable Data Breach Scheme** Under Part IIIC of the Privacy Act, the notifiable data breach scheme (NDB scheme) requires an APP entity to notify individuals and the Australian Information Commissioner where there has been an unauthorised access, disclosure or loss of personal information that a reasonable person would conclude

		is likely to result in serious harm to an individual (some limited exceptions apply). The Information Commissioner administers the NDB scheme and has powers to investigate and regulate non-compliance.

ACCESS AND CORRECTION

Assessment Purpose - *The questions in this section are directed towards ensuring that individuals are able to access and correct their information. This section includes specific conditions for what would be considered reasonable in the provision of access. Access will also be conditioned by security requirements that preclude the provision of direct access to information and will require sufficient proof of identity prior to provision of access. The details of the procedures whereby the ability to access and correct information is provided may differ depending on the nature of the information and other interests, which is why, in certain circumstances, it may be impossible, impracticable or unnecessary to change, suppress or delete records.*

The ability to access and correct personal information, while generally regarded as a central aspect of privacy protection, is not an absolute right. While you should always make good faith efforts to provide access, in some situations, it may be necessary to deny claims for access and correction. Section II of the CBPR Self-Assessment Guidelines for Organisations sets out those conditions that must be met in order for such denials to be considered acceptable. When you deny a request for access, for the reasons specified herein, you should provide the requesting individual with an explanation as to why you have made that determination and information on how to challenge that denial. You would not be expected to provide an explanation, however, in cases where such disclosure would violate a law or judicial order. Refer to the APEC Cross Border Privacy Rules Intake Questionnaire for a list of acceptable Qualifications to the provision of access and correction mechanisms.

Question (*to be answered by the Applicant*)	Assessment Criteria (*to be verified by the Accountability Agent*)	Enforceability (*to be answered by the Economy*)
36. Upon request, do you provide confirmation of whether or not you hold personal information about the requesting individual? Describe below.	Where the Applicant answers YES, the Accountability Agent must verify that the Applicant has procedures in place to respond to such requests. The Applicant must grant access to any individual, to personal information collected or gathered about that individual, upon receipt of sufficient information confirming the individual's identity. The Applicant's processes or mechanisms	APP 1, 5 and 12 APP 1 APP 1 requires an entity to have a clearly expressed and up-to-date policy that includes: • the kinds of personal information that the entity collects and holds; and • how an individual may access personal information about the individual that is held by the entity and seek the correction of such information.

	for access by individuals to personal information must be reasonable having regard to the manner of request and the nature of the personal information. The personal information must be provided to individuals in an easily comprehensible way. The Applicant must provide the individual with a time frame indicating when the requested access will be granted. Where the Applicant answers NO and does not identify an applicable qualification, the Accountability Agent must inform the Applicant that the existence of written procedures to respond to such requests is required for compliance with this principle. Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.	APP 5 requires an APP entity that collects personal information to take such steps (if any) as are reasonable in the circumstances to notify the individual of certain matters, which include: - the identity and contact details of the APP entity; - the purpose for which the APP entity collects the personal information; and - 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 (as contained within the entity's privacy policy, required by APP 1. APP 12 If an APP entity holds personal information about an individual, APP 12 requires the entity, on request by the individual, to give the individual access to the information. An APP entity may refuse to give access if required or authorised to refuse access under an Australian law (APP 12.2 and 12.3(g)). An organisation may refuse to give access if any of the ten criteria listed in APP 12.3 are made out. These exceptions relate to protecting the safety of the public, the

		privacy of individuals, and the integrity of law enforcement related activities or legal proceedings. The access may also be refused if the request is frivolous or vexatious or giving access would reveal commercially sensitive information about the organisation.
37. Upon request, do you provide individuals access to the personal information that you hold about them? Where YES, answer questions 37(a) – (e) and describe your applicant's policies/procedures for receiving and handling access requests. Where NO, proceed to question 38. 37.a) Do you take steps to confirm the identity of the individual requesting access? If YES, please describe. 37.b) Do you provide access within a reasonable time frame following an individual's request for access? If YES, please describe. 37.c) Is information communicated in a reasonable manner that is generally understandable (in a legible format)? Please describe. 37.d) Is information provided in a way that is compatible with the regular form of	Where the Applicant answers YES the Accountability Agent must verify each answer provided. The Applicant must implement reasonable and suitable processes or mechanisms to enable the individuals to access their personal information, such as account or contact information. If the Applicant denies access to personal information, it must explain to the individual why access was denied, and provide the appropriate contact information for challenging the denial of access where appropriate. Where the Applicant answers NO and does not identify an applicable qualification, the Accountability Agent must inform the Applicant that it may be required to permit access by individuals to their personal information. Where the Applicant identifies an applicable	APP 12 An APP entity must be satisfied that a request for personal information under APP 12 is made by the individual concerned, or by another person who is authorised to make a request on their behalf, for example, as a legal guardian or authorised agent. If an entity gives access to the personal information of another person, this could constitute a disclosure, which may not comply with APP 6. The steps appropriate to verify an individual's identity will depend on the circumstances. In particular, whether the individual is already known to or readily identifiable by the APP entity, the sensitivity of the personal information and the possible adverse consequences for the individual of unauthorised disclosure. The minimum amount of personal information needed to establish an individual's identity should be sought.

interaction with the individual (e.g. email, same language, etc)? 37.e) Do you charge a fee for providing access? If YES, describe below on what the fee is based and how you ensure that the fee is not excessive.	qualification, the Accountability Agent must verify whether the applicable qualification is justified.	In accordance with APP 12.4, the APP entity must: - respond to the request for access to the personal information within 30 days if the entity is a government agency; and within a reasonable period if the entity is an organisation; and - give access to the information, or in the manner requested by the individual, if it is reasonable and practicable to do so. If the APP entity refuses to give access due to subclause 12.2 or 12.3 or 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. Upon refusal, the entity must give the individual a written notice that sets out the reasons for the refusal (unless it would be unreasonable to do so), and the mechanisms available to complain about the refusal (APP 12.9). An APP entity must give access to personal information in the manner requested by the individual, if it is reasonable and practicable to do so (APP

		12.4(b)). The manner of access may, for example, be by email, by phone, in person, hard copy, or an electronic record. If the APP entity is a government agency, the entity must not charge the individual for the making of the request or for giving access to the personal information (APP 12.7). If the APP entity is an organisation and charges the individual for giving access to said information, the charge must not be excessive and must not apply to the making of the request (APP 12.8).
38. Do you permit individuals to challenge the accuracy of their information, and to have it rectified, completed, amended and/or deleted? Describe your applicant's policies/procedures in this regard below and answer questions 37 (a), (b), (c), (d) and (e). 38.a) Are your access and correction mechanisms presented in a clear and conspicuous manner? Provide a description in the space below or in an attachment if necessary. 38.b) If an individual demonstrates that personal information about them is	Where the Applicant answers YES to questions 38.a, the Accountability Agent must verify that such policies are available and understandable in the primarily targeted economy. If the Applicant denies correction to the individual's personal information, it must explain to the individual why the correction request was denied, and provide the appropriate contact information for challenging the denial of correction where appropriate. All access and correction mechanisms have to be simple and easy to use, presented in a clear and visible manner,	APP 1, 5,10, 13 APP 1 An APP entity is also required by APP 1.4(d) to state in an APP Privacy Policy how an individual may seek the correction of their personal information held by the entity. APP 5 An APP entity is required by APP 5.2(g) to take reasonable steps to notify an individual, or ensure they are aware, of the fact the entity's APP Privacy Policy contains information about how the individual may seek correction of their personal information held by the entity. An APP entity is obliged to take such

incomplete or incorrect, do you make the requested correction, addition, or where appropriate, deletion? 38.c) Do you make such corrections or deletions within a reasonable time frame following an individual's request for correction or deletion? 38.d) Do you provide a copy to the individual of the corrected personal information or provide confirmation that the data has been corrected or deleted? 38.e) If access or correction is refused, do you provide the individual with an explanation of why access or correction will not be provided, together with contact information for further inquiries about the denial of access or correction?	operate within a reasonable time frame, and confirm to individuals that the inaccuracies have been corrected, amended or deleted. Such mechanisms could include, but are not limited to, accepting written or e-mailed information requests, and having an employee copy the relevant information and send it to the requesting individual. Where the Applicant answers NO to questions 38a-38e and does not identify an applicable qualification, the Accountability Agent must inform the Applicant that the existence of written procedures to respond to such requests is required for compliance with this principle. Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.	steps (if any) as are reasonable in the circumstances to ensure that the personal information that the entity collects, uses or discloses is, having regard to the purpose of the use or disclosure, accurate, up-to-date complete and relevant. APP 10 APP 10 provides that an APP entity must take reasonable steps to ensure the quality of personal information it collects, uses or discloses (APP 10). If reasonable steps are taken to comply with APP 10, this reduces the likelihood that personal information will need correction (under APP 13) APP 13 APP 13 requires an APP entity to 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. This requirement applies where: - the APP entity is satisfied the personal information is inaccurate, out-of-date, incomplete, irrelevant or misleading, having regard to a purpose for which it is held, or - the individual requests the entity

		to correct the personal information In accordance with APP 13.5, the APP entity must: - respond to the request within 30 days if the entity is a government agency or within a reasonable period if the entity is an organisation; and - not charge the individual for making the request, for correcting the personal information or for associating the statement with the personal information. 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 the reasons for the refusal (unless it would be unreasonable to do so), and the mechanisms available to complain about the refusal (APP 13.3). In particular, the individual should be advised that: - a complaint should first be made in writing to the APP entity (s 40(1A)) - the entity should be given a reasonable time (usually 30 days) to respond - a complaint may then be taken to a recognised external dispute resolution scheme of which the entity is a

		member (if any), and - lastly, that a complaint may be made to the Australian Information Commissioner (s 36). If an APP entity refuses a request to correct personal information, the individual can request 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 (APP 13.4).

ACCOUNTABILITY

Assessment Purpose - *The questions in this section are directed towards ensuring that the Applicant is accountable for complying with measures that give effect to the other Principles stated above. Additionally, when transferring information, the Applicant should be accountable for ensuring that the recipient will protect the information consistently with these Principles when not obtaining consent. Thus, you should take reasonable steps to ensure the information is protected, in accordance with these Principles, after it is transferred. However, there are certain situations where such due diligence may be impractical or impossible, for example, when there is no on-going relationship between you and the third party to whom the information is disclosed. In these types of circumstances, you may choose to use other means, such as obtaining consent, to assure that the information is being protected consistently with these Principles. However, in cases where disclosures are required by domestic law, you would be relieved of any due diligence or consent obligations.*

Question (*to be answered by the Applicant*)	Assessment Criteria (*to be verified by the Accountability Agent*)	Enforceability (*to be answered by the Economy*)
39. What measures do you take to ensure compliance with the APEC Information Privacy Principles? Please check all that apply and describe. Internal guidelines or policies (if applicable, describe how implemented) _____ Contracts _____ Compliance with applicable industry or sector laws and regulations ____ Compliance with self-regulatory applicant code and/or rules ____ Other (describe) ____	The Accountability Agent has to verify that the Applicant indicates the measures it takes to ensure compliance with the APEC Information Privacy Principles.	The Office of the Australian Information Commissioner (OAIC), established by the *Australian Information Commissioner Act 2010*, is responsible for investigating breaches and possible breaches of the APPs and the Privacy Act. The specific prescriptive provisions of the CBPR could become more explicitly enforceable through the adoption of a binding APP code developed by the Information Commissioner (Part IIIB). A breach of a code would be a breach of the Privacy Act. The Australian Competition and Consumer Commission is Australia's peak consumer protection and competition agency. Section 18 of the Australian Consumer Law prohibits misleading or deceptive conduct. By joining the APEC CBPR, a company commits to comply the program requirements. Failure to comply may constitute misleading or deceptive conduct, which may lead to enforcement action under section 18.
40. Have you appointed an individual(s) to	Where the Applicant answers YES, the	The Office of the Australian Information

be responsible for your overall compliance with the Privacy Principles?	Accountability Agent must verify that the Applicant has designated an employee(s) who is responsible for the Applicant's overall compliance with these Principles. The Applicant must designate an individual or individuals to be responsible for the Applicant's overall compliance with privacy principles as described in its Privacy Statement, and must implement opportune procedures to receive, investigate, and respond to privacy-related complaints, providing an explanation of any remedial action where applicable. Where the Applicant answers NO, the Accountability Agent must inform the Applicant that designation of such an employee(s) is required for compliance with this principle.	Commissioner (OAIC), established by the *Australian Information Commissioner Act 2010*, is responsible for investigating breaches and possible breaches of the APPs and the Privacy Act. The specific prescriptive provisions of the CBPR could become more explicitly enforceable through the adoption of a binding code developed by the Information Commissioner (Part IIIB). A breach of a code would be a breach of the Privacy Act. APP 1 imposes three separate obligations upon an APP entity to: - take reasonable steps to implement practices, procedures and systems that will ensure the entity complies with the APPs and any binding registered APP code, and is able to deal with related inquiries and complaints (APP 1.2) - have a clearly expressed and up-to-date APP Privacy Policy about how the entity manages personal information (APP 1.3 and 1.4) - take reasonable steps to make its APP Privacy Policy available free of charge in an appropriate form (APP 1.5) and,

		upon request, in a particular form (APP 1.6). The Australian Government agencies Privacy Code (the Code) commences on 1 July 2018. It requires Australian Government agencies subject to the Privacy Act to appoint a Privacy Officer and a Privacy Champion to undertake particular functions and roles (sections 10 and 11).
41. Do you have procedures in place to receive, investigate and respond to privacy-related complaints? Please describe.	Where the Applicant answers YES, the Accountability Agent must verify that the Applicant has procedures in place to receive, investigate and respond to privacy-related complaints, such as: 1) A description of how individuals may submit complaints to the Applicant (e.g. Email/Phone/Fax/Postal Mail/Online Form); AND/OR 2) A designated employee(s) to handle complaints related to the Applicant's compliance with the APEC Privacy Framework and/or requests from individuals for access to personal information; AND/OR 3) A formal complaint-resolution process; AND/OR	APP 1, 5 An APP entity must include in its APP Privacy Policy information about: - how an individual may complain if the entity breaches the APPs or any registered binding APP code, and how the complaint will be handled (APP 1.4(e)). APP 5 An APP entity must take reasonable steps at or before the time of collection of personal information to notify the individual of certain matters, including: - How the individual may complain about a breach of the APPs and how an entity will deal with such complaint (APP5.2(h)).

	4) Other (must specify). Where the Applicant answers NO, the Accountability Agent must inform the Applicant that implementation of such procedures is required for compliance with this principle.	The Office of the Australian Information Commissioner (OAIC), established by the *Australian Information Commissioner Act 2010*, is responsible for receiving privacy complaints and investigating breaches and possible breaches of the APPs and the Privacy Act. Before lodging a complaint with the OAIC, the individual would generally need to complain directly to the agency or organisation and allow 30 days for it to respond. If no response is received within that time, or the individual is dissatisfied with the response, they may then complain to the OAIC (s 36). Complaints to the OAIC must be made in writing. It is free to lodge a complaint with the OAIC. The Commissioner has a range of powers relating to the conduct of investigations including powers: • to conciliate complaints (s 40A); and • to make preliminary inquiries of any person (s 42); and

		• to require a person to give information or documents, or to attend a compulsory conference (ss 44-47); and • to transfer matters to an alternative complaint body in certain circumstances (s 49).
42. Do you have procedures in place to ensure individuals receive a timely response to their complaints?	Where the Applicant answers YES, the Accountability Agent must verify that the Applicant has procedures in place to ensure individuals receive a timely response to their complaints. Where the Applicant answers NO, the Accountability Agent must inform the Applicant that implementation of such procedures is required for compliance with this principle.	The Office of the Australian Information Commissioner (OAIC), established by the *Australian Information Commissioner Act 2010*, is responsible for receiving privacy complaints and investigating breaches and possible breaches of the APPs and the Privacy Act.
43. If YES, does this response include an explanation of remedial action relating to their complaint? Describe.	The Accountability Agent must verify that the Applicant indicates what remedial action is considered.	The Office of the Australian Information Commissioner (OAIC), established by the *Australian Information Commissioner Act 2010*, is responsible for receiving privacy complaints and investigating breaches and possible breaches of the APPs and the Privacy Act. APP 1 APP 1 requires an entity to take such steps as are reasonable in the circumstances to

		implement practices, procedures and systems relating to the entity's functions or activities that: - will ensure that the entity complies with the APPs and a registered APP code (if any) that binds the entity; and - will enable the entity to deal with inquiries or complaints from individuals about the entity's compliance with the APPs or such a code.
44. Do you have procedures in place for training employees with respect to your privacy policies and procedures, including how to respond to privacy-related complaints? If YES, describe.	Where the Applicant answers YES, the Accountability Agent must verify that the Applicant has procedures regarding training employees with respect to its privacy policies and procedures, including how to respond to privacy-related complaints. Where the Applicant answers that it does not have procedures regarding training employees with respect to their privacy policies and procedures, including how to respond to privacy-related complaints, the Accountability Agent must inform the Applicant that the existence of such procedures is required for compliance with this principle.	The Office of the Australian Information Commissioner (OAIC), established by the *Australian Information Commissioner Act 2010*, is responsible for receiving privacy complaints and investigating breaches and possible breaches of the APPs and the Privacy Act. APP 1 APP 1 requires an entity to take such steps as are reasonable in the circumstances to implement practices, procedures and systems relating to the entity's functions or activities that: - will ensure that the entity complies with the APPs and a registered APP code (if any) that binds the entity; and - will enable the entity to deal with

		inquiries or complaints from individuals about the entity's compliance with the APPs or such a code.
45. Do you have procedures in place for responding to judicial or other government subpoenas, warrants or orders, including those that require the disclosure of personal information?	Where the Applicant answers YES, the Accountability Agent must verify that the Applicant has procedures in place for responding to judicial or other government subpoenas, warrants or orders, including those that require the disclosure of personal information, as well as provide the necessary training to employees regarding this subject. Where the Applicant answers NO, the Accountability Agent must inform the Applicant that such procedures are required for compliance with this principle.	The Office of the Australian Information Commissioner (OAIC), established by the *Australian Information Commissioner Act 2010*, is responsible for receiving privacy complaints and investigating breaches and possible breaches of the APPs and the Privacy Act. APP 6 APP 6 outlines when an APP entity may use or disclose personal information. An APP entity can only use or disclose personal information for a purpose for which it was collected (known as the 'primary purpose'), or for a secondary purpose if an exception applies. In relation to responding to judicial or other government subpoenas, warrants or orders a relevant exception applies where: - the secondary use or disclosure is required or authorised by or under an Australian law or a court/tribunal order (APP 6.2(b))
46. Do you have mechanisms in place with personal information processors, agents,	Where the Applicant answers YES, the Accountability Agent must verify the	The Office of the Australian Information Commissioner (OAIC), established by the *Australian Information Commissioner Act*

contractors, or other service providers pertaining to personal information they process on your behalf, to ensure that your obligations to the individual will be met (check all that apply)? Internal guidelines or policies _____ Contracts _____ Compliance with applicable industry or sector laws and regulations _____ Compliance with self-regulatory applicant code and/or rules _____ Other (describe) _____	existence of each type of agreement described. Where the Applicant answers NO, the Accountability Agent must inform the Applicant that implementation of such agreements is required for compliance with this principle.	*2010*, is responsible for receiving privacy complaints and investigating breaches and possible breaches of the APPs and the Privacy Act. A government agency entering into a Commonwealth contract must take contractual measures to ensure that the other party (the contracted service provider) does not do an act, or engage in a practice, that would breach an APP if done or engaged in by the agency (s 95B). In effect, s 95B ensures that the contracted service provider complies with the APPs as if it were a government agency in respect of its activities under the contract. APP 8 APP 8 deals with overseas disclosure of personal information held in Australia. APP 8 generally requires an APP entity, before disclosing personal information to an overseas recipient, such as a subcontractor, to take reasonable steps to ensure that overseas recipient will handle the personal information in accordance with the APPs. Importantly, the APPs include a requirement for businesses to take reasonable steps to protect personal information from unauthorised access or

		disclosure (APP 11.1(b)). Section 16C of the Privacy Act makes the Australian APP entity responsible for personal information disclosed to an overseas recipient, unless an exception applies. This means the Australian APP entity will be accountable if the overseas entity mishandles the information.
47. Do these agreements generally require that personal information processors, agents, contractors or other service providers: Abide by your APEC-compliant privacy policies and practices as stated in your Privacy Statement? _____ Implement privacy practices that are substantially similar to your policies or privacy practices as stated in your Privacy Statement? _____ Follow instructions provided by you relating to the manner in which your personal information must be handled? _____ Impose restrictions on subcontracting unless with your consent? _____ Have their CBPRs certified by an APEC accountability agent in their jurisdiction?	The Accountability Agent must verify that the Applicant makes use of appropriate methods to ensure their obligations are met.	The Office of the Australian Information Commissioner (OAIC), established by the *Australian Information Commissioner Act 2010*, is responsible for receiving privacy complaints and investigating breaches and possible breaches of the APPs and the Privacy Act. The specific prescriptive provisions of the CBPR could become more explicitly enforceable through the adoption of a binding code developed by the Information Commissioner (Part IIIB). A breach of a code would be a breach of the Privacy Act.

_____ □ Notify the Applicant in the case of a breach of the personal information of the Applicant's customers? □ Other (describe) _____		
48. Do you require your personal information processors, agents, contractors or other service providers to provide you with self-assessments to ensure compliance with your instructions and/or agreements/contracts? If YES, describe below.	The Accountability Agent must verify the existence of such self-assessments.	The Office of the Australian Information Commissioner (OAIC), established by the *Australian Information Commissioner Act 2010*, is responsible for receiving privacy complaints and investigating breaches and possible breaches of the APPs and the Privacy Act. The specific prescriptive provisions of the CBPR could become more explicitly enforceable through the adoption of a binding code developed by the Information Commissioner (Part IIIB). A breach of a code would be a breach of the Privacy Act.
49. Do you carry out regular spot checking or monitoring of your personal information processors, agents, contractors or other service providers to ensure compliance with your instructions and/or agreements/contracts? If YES, describe.	Where the Applicant answers YES, the Accountability Agent must verify the existence of the Applicant's procedures such as spot checking or monitoring mechanisms. Where the Applicant answers NO, the Accountability Agent must require the	The Office of the Australian Information Commissioner (OAIC), established by the *Australian Information Commissioner Act 2010*, is responsible for receiving privacy complaints and investigating breaches and possible breaches of the APPs and the Privacy Act.

	Applicant to describe why it does not make use of such spot checking or monitoring mechanisms.	The specific prescriptive provisions of the CBPR could become more explicitly enforceable through the adoption of a binding code developed by the Information Commissioner (Part IIIB). A breach of a code would be a breach of the Privacy Act.
50. Do you disclose personal information to other recipient persons or organizations in situations where due diligence and reasonable steps to ensure compliance with your APEC CBPRs by the recipient as described above is impractical or impossible?	If YES, the Accountability Agent must ask the Applicant to explain: (1) why due diligence and reasonable steps consistent with the above Assessment Criteria for accountable transfers are impractical or impossible to perform; and (2) the other means used by the Applicant for ensuring that the information, nevertheless, is protected consistent with the APEC Privacy Principles. Where the Applicant relies on an individual's consent, the Applicant must explain to the satisfaction of the Accountability Agent the nature of the consent and how it was obtained.	The Office of the Australian Information Commissioner (OAIC), established by the *Australian Information Commissioner Act 2010*, is responsible for receiving privacy complaints and investigating breaches and possible breaches of the APPs and the Privacy Act. APP 6 An APP entity can only use or disclose personal information for a purpose for which it was collected (known as the 'primary purpose'), or for a secondary purpose if an exception applies (APP 6). The exceptions include where: - the individual has consented to a secondary use or disclosure o consent is defined in s 6(1) as express consent or implied consent - the individual would reasonably expect the APP entity to use or disclose their personal information

		for the secondary purpose, and that purpose is related to the primary purpose of collection, or, in the case of sensitive information, directly related to the primary purpose - the secondary use or disclosure is required or authorised by or under an Australian law or a court/tribunal order - a permitted general situation exists in relation to the secondary use or disclosure - the APP entity is an organisation and a permitted health situation exists in relation to the secondary use or disclosure - the APP entity reasonably believes that the secondary use or disclosure is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body, or - the APP entity is a government agency (other than an enforcement body) and discloses biometric information or biometric templates to an enforcement body, and the disclosure is conducted in accordance with guidelines made by the Information Commissioner for the purposes of APP 6.3.

		APP 11 APP entity must take reasonable steps to protect the personal information it holds, including from interference, loss and unauthorised modification (APP 11.1). The term ‘holds’ extends beyond physical possession of a record to include a record that an APP entity has the right or power to deal with. For example, an entity that outsources the storage of personal information to a third party, but retains the right to deal with that information, including to access and amend it, holds that personal information.