

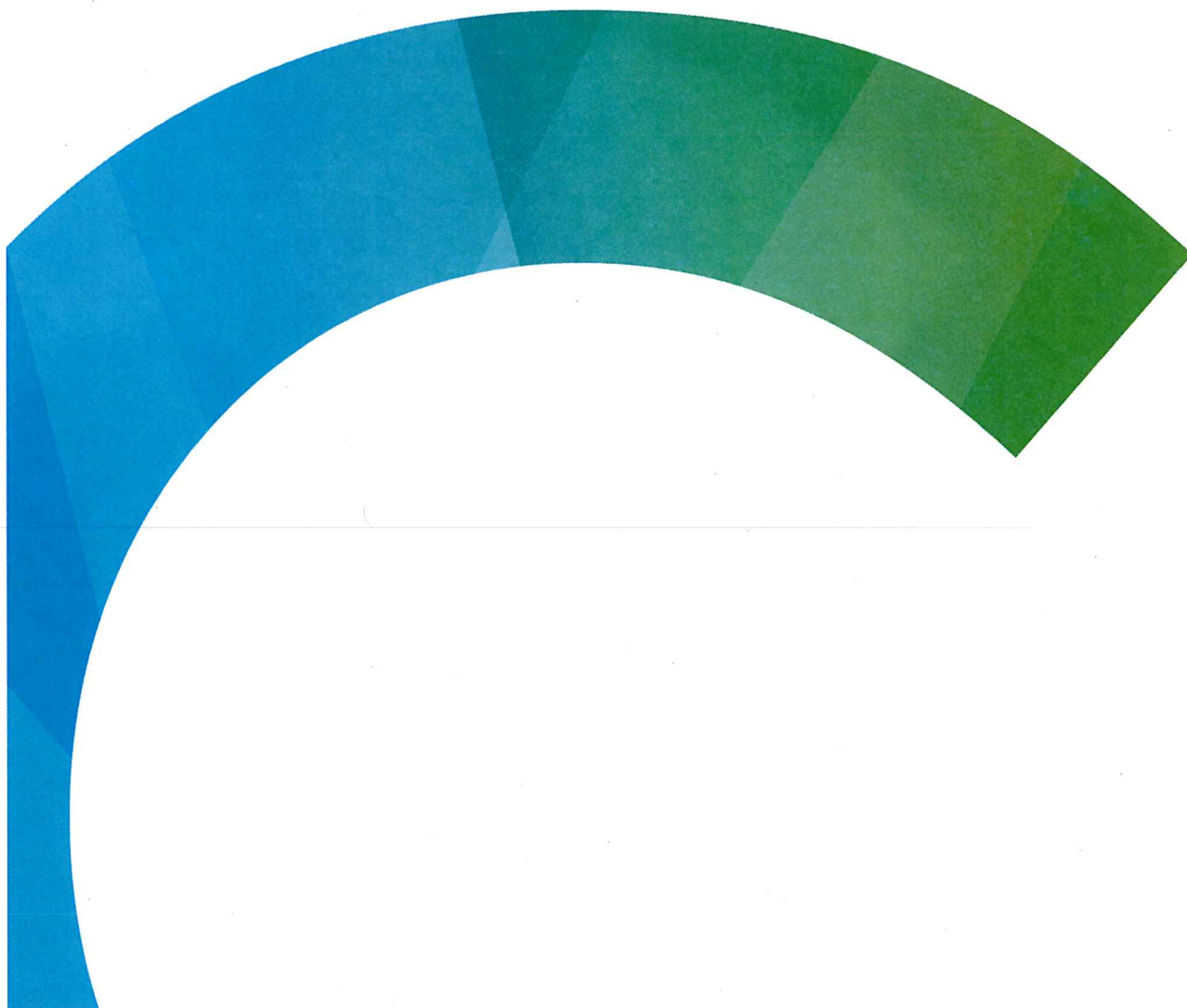


Australian Government
Climate Change Authority

CLIMATE CHANGE AUTHORITY PRIVACY POLICY

Corporate Policy

MARCH 2014



Foreward

The Climate Change Authority (**we, our, us, the Authority**) recognises the importance of protecting your privacy and personal information. As an Australian Government Agency, the Authority is bound by the Australian Privacy Principles (APPs) in the [Privacy Act 1988](#) (Cth) (the Privacy Act), which regulates how agencies collect, use, disclose and store personal information, including sensitive information, and how individuals may access and correct records containing their personal information. We respect your rights to privacy under the Privacy Act and we comply with all the Privacy Act's requirements in respect of the collection and management of your personal information.

This document is our privacy policy and it tells you how we collect, use, store and disclose your personal information and the way in which you can access and correct your personal information.

TABLE OF CONTENTS

TABLE OF CONTENTS	II
CHAPTER 1. GENERAL INFORMATION	3
1. What personal information we collect	3
2. How we collect your personal information	3
3. How we collect, hold, use and disclose your personal information	4
4. To whom we may disclose your information	4
5. Cloud Computing	4
6. Security	5
7. How you can access and correct your personal information	5
8. How to contact us about a possible breach of privacy	5
9. Contacting us	6
10. Changes to our privacy policy	6
CHAPTER 2. AUSTRALIAN PRIVACY PRINCIPLES (APPS)	7
11. CONSIDERATION OF PERSONAL INFORMATION PRIVACY	7
11.1. APP 1 – Open and transparent management of personal information	7
11.2. APP 2 – Anonymity and pseudonymity	8
12. COLLECTION OF PERSONAL INFORMATION	8
12.1. APP 3 – Collection of solicited information	8
12.2. APP 4 – Dealing with unsolicited personal information	9
12.3. APP 5 – Notification of collection of personal information	9
13. DEALING WITH PERSONAL INFORMATION	9
13.1. APP 6 – Use or disclosure of personal information	9
13.2. APP 7 – Direct Marketing	10
13.3. APP 8 – Cross-border disclosure of personal information	10
13.4. APP 9 – Adoption, use or disclosure of government related identifiers	10
14. INTEGRITY OF PERSONAL INFORMATION	10
14.1. APP 10 – Quality of personal information	10
14.2. APP 11 – Security of personal information	11
15. ACCESS TO, AND CORRECTION OF, PERSONAL INFORMATION	11
15.1. APP 12 – Access to personal information	11
15.2. APP 13 – Correction of personal information	11

CHAPTER 1. GENERAL INFORMATION

1. What personal information we collect

The Authority collects personal information that is reasonably necessary for, or directly related to, its functions and activities. The Authority will only use and disclose your personal information for the purposes it was collected and in accordance with the Privacy Act.

When used in this privacy policy, the term “personal information” has the meaning given to it in the Privacy Act. In general terms, it is any information that can be used to identify you whether or not the information is true. If the information we collect identifies you, or your identity can be reasonably ascertained from it, the information will be considered personal information.

The type of personal information we may collect includes, but is not limited to:

- name;
- mailing and/or street address;
- email address;
- telephone contact number;
- facsimile number;
- age and/or birth date;
- profession, occupation and/or job title;
- sensitive information as defined by the Privacy Act (such as information about ethnicity);
- photographic images and/or pictorial representations;
- any additional information relating to you that you provide to us directly through our website or indirectly through use of our website, through our representatives or otherwise; and
- information you provide to us through surveys or visits by our representatives from time to time.

Business information provided to the Authority will not ordinarily fall within the definition of personal information under the Privacy Act but it may do so when the business information relates to sole traders and partnerships.

In circumstances where it will be impracticable for the Authority to deal with you anonymously, or through the use of a pseudonym, the Authority will ordinarily request you to identify yourself to enable the Authority to appropriately carry out its functions and activities.

2. How we collect your personal information

When collecting personal information, we may collect it in ways including, but not limited to:

- directly from you, through your access and use of our website and web based channels;
- during conversations with you and our representatives via telephone and in person;
- through written correspondence with you, including correspondence via email; and
- when you complete an application.

From time to time, we may also collect personal information from third parties including, but not limited to:

- other government agencies; law enforcement agencies; credit reporting agencies and service providers to the Authority.



Collection of personal information from a third party or a private source will only be carried out by the Authority if you consent; the Authority is required or authorised to collect the information under an Australian law, or a court/tribunal order; or if it is reasonable or practicable for us to collect information in this way.

In limited circumstances, the Authority may receive personal information about third parties from individuals who contact us or supply us with personal information belonging to others in the documents they provide. This is referred to as 'unsolicited personal information'. In these circumstances we will consider whether the Authority could have collected the information had it solicited the information, and will handle it in accordance with the Privacy Act.

3. How we collect, hold, use and disclose your personal information

We collect personal information about you so that we can perform our functions and activities.

We collect, hold, use and disclose your personal information to:

- identify you;
- to send communications requested by you;
- answer enquiries, and provide information or advice;
- conduct business processing functions;
- update our records and keep your contact details up-to-date;
- process and respond to any complaint made by you;
- conduct planning; report evaluation; quality control and research for the purposes of the Authority, its contractors or service providers;
- provide information to our contractors or service providers to enable them to provide our products and services to you; and
- comply with any Australian law; orders of courts or tribunals; any rule, regulation, lawful and binding determination, decision or direction of a regulator; or in co-operation with any governmental authority of any country (or political sub-division of a country).

4. To whom we may disclose your information

The third parties we may disclose your personal information to include, but are not limited to:

- our employees, contractors or service providers for the purposes of the operation of our functions, fulfilling requests by you, and to otherwise provide information, products and services to you including, without limitation, web hosting providers, IT systems administrators, cloud computing services, mailing houses, couriers, payment processors, data entry service providers, electronic network administrators, debt collectors, and professional advisors such as accountants, solicitors, business advisors and consultants;
- other Commonwealth, State or Territory government Authorities and agencies where it is authorised by law or is established practice; and
- any organisation for any authorised purpose with your express consent.

Your personal information will not be shared or disclosed other than as described in this privacy policy, without your consent.

5. Cloud Computing

The Authority complies with its cloud computing obligations in accordance with the guidelines issued by the Attorney-General. For further information, please refer to the [Policy and Risk Management Guidelines for the Storage and Processing of Australian Government Information in outsourced or offshore ICT arrangements](#).

6. Security

Once the Authority receives information from you, the information is maintained in a secure environment. Your personal information will not be released unless the law permits it or your permission is granted.

We take reasonable steps to ensure your personal information is protected from misuse and loss and from unauthorised access, modification or disclosure. We may hold your information in either electronic or hard copy form. Personal information is destroyed or de-identified when no longer needed in accordance with the requirements of the *Archives Act 1983* (Cth).

However, as our website is linked to the internet, and we cannot provide assurance regarding the security of transmission of information you communicate to us. We also cannot guarantee that the information you supply will not be intercepted while being transmitted over the internet. Any personal information or other information which you send to us is transmitted at your own risk.

Our website may contain links to other websites operated by third parties. We make no representations or warranties in relation to the privacy practices of any third party website and we are not responsible for the privacy policies or the content of any third party website. Third party websites are responsible for informing you about their own privacy practices. The Authority encourages you to examine each website's privacy policy.

If you have concern in this regard, the Authority has other ways of obtaining and providing information (e.g. mail, telephone and facsimile facilities are available).

7. How you can access and correct your personal information

You may request access to any personal information we hold about you at any time by contacting us. Where we hold information that you are entitled to access, we will provide you with suitable means of accessing it (e.g. by mailing or emailing it to you). We will not charge you for providing the information to you, or for the costs of making any corrections to your personal information.

If you believe that personal information we hold about you is incorrect, incomplete or inaccurate, then you may request to have it amended. We will consider whether the information requires amendment. In the unlikely event that we do not agree that there are grounds for amendment, we will give you written notice of the reasons for the refusal within 30 days of receipt of your request, together with information about mechanisms available to seek review if you do not agree with our decision.

There may be instances where we cannot grant you access to the personal information we hold. For example, we may need to refuse access if required or authorised to refuse access under Commonwealth legislation. If that happens, we will give you written notice of the reasons for the refusal within 30 days of receipt of your request, together with information about how you can complain about our refusal if you wish to do so.

8. How to contact us about a possible breach of privacy

If you believe that we have breached your privacy, please contact us using the contact information below and provide details of the incident so that we can investigate it.

When a complaint is received, the Authority will conduct internal enquiries into the possible breach. The Authority will deal with your complaint as quickly as possible and keep you informed of its progress. Once the Authority has completed its internal enquiries, you will be advised of the outcome in writing.



If you are not happy with the response provided by the Authority, you can make a complaint to the Office of the Australian Information Commissioner (OAIC). Information on how to make a complaint can be found on the [OAIC website](#).

9. Contacting us

If you have any questions about this privacy policy, any concerns or a complaint regarding the treatment of your privacy or a possible breach of your privacy, please use the Contact link on our website or contact our Privacy Officer via the details set out below.

Requests and complaints will be treated confidentially. Our representative will contact you within a reasonable time after receipt of your complaint to discuss your concerns and outline options regarding how they may be resolved. We will aim to ensure that your complaint is resolved in a timely and appropriate manner. Please contact our Privacy Officer at:

Privacy Officer

Climate Change Authority
GPO Box 1944
Melbourne City VIC 3000

Facsimile: 03 8656 3030

Email: privacy@climatechangeauthority.gov.au

10. Changes to our privacy policy

We may change this privacy policy from time to time. Any updated versions of this privacy policy will be posted on our website.

This privacy policy was last updated on 31 March 2014.

CHAPTER 2. AUSTRALIAN PRIVACY PRINCIPLES (APPS)

The 13 APPs are divided into five different parts according to their different stages of personal information management running from the collection of personal information through to its disposal.

A summary of the APP's is provided below. The full text of the APPs can be found in Schedule 1 of the [Privacy Act 1988](#).

Part 1: Consideration of personal information privacy

- APP 1 – Open and transparent management of personal information
- APP 2 – Anonymity and pseudonymity

Part 2: Collection of personal information

- APP 3 – Collection of solicited personal information
- APP 4 – Dealing with unsolicited personal information
- APP 5 – Notification of collection of personal information

Part 3: Dealing with personal information

- APP 6 – Use or disclosure of personal information
- APP 7 – Direct marketing
- APP 8 – Cross-border disclosure of personal information
- APP 9 – Adoption, use and disclosure of government related identifiers

Part 4: Integrity of personal information

- APP 10 – Quality of personal information
- APP 11 – Security of personal information

Part 5: Access to, and correction of, personal information

- APP 12 – Access to personal information
- APP 13 – Correction of personal information

11. CONSIDERATION OF PERSONAL INFORMATION PRIVACY

11.1. APP 1 – Open and transparent management of personal information

APP 1 requires APP entities to manage personal information in an open and transparent way. This includes agencies being required to:

- take reasonable steps to implement practices, procedures and systems relating to the agency's functions or activities that will ensure compliance with the APPs (APP 1.2);
- have a clearly expressed and up-to-date privacy policy about the management of personal information (APP 1.3) that specifies:
 - the kinds of personal information collected;
 - how personal information is collected and held;
 - how an individual may seek access to personal information held by the agency or seek correction of such information;



- how an individual may complain about a breach of an APP and how the agency will deal with such a complaint;
- whether the agency is likely to disclose personal information to overseas recipients and if so, the countries in which such recipients are likely to be located, if it is practicable to specify those countries (APP 1.4);
- take reasonable steps to make its privacy policy available free of charge and in the appropriate form, such as on the agency's website (APP 1.5); and
- take reasonable steps to give a copy of the agency's privacy policy in a particular form, if requested by an individual or body (APP 1.6).

11.2. APP 2 – Anonymity and pseudonymity

APP 2.1 provides that individuals must have the option of dealing with an agency anonymously or through the use of a pseudonym in relation to a particular matter unless:

- the agency is required or authorised by or under an Australian law or a court/tribunal order to deal with individuals who have identified themselves; or
- it is impracticable for the agency to deal with individuals who have not identified themselves.

Due to the nature of the programs administered by the Department, it will ordinarily be impracticable to deal with individuals anonymously or through the use of a pseudonym. Accordingly, the Department will ordinarily request that an individual identify themselves in order for the Department to appropriately carry out its functions and activities.

12. COLLECTION OF PERSONAL INFORMATION

12.1. APP 3 – Collection of solicited information

APP 3 applies to personal information solicited by an agency. APP 3.1 provides that an agency must not collect personal information unless the information is reasonably necessary for, or directly related to, at least one of the agency's functions or activities.

APP 3.3 provides that an agency must not collect *sensitive information* about an individual unless one of the exemptions in APP 3.4 applies, or:

- the individual consents to the collection of the information; and
- the information is reasonably necessary for at least one of the agency's functions or activities.

The exemptions in APP 3.4 include where the collection of sensitive information is required or authorised under an Australian law or a court/tribunal order.

The definition of sensitive information, found in section 6 of the Privacy Act, includes (but is not limited to) information or opinion about an individual's racial or ethnic origin, political opinions, religious beliefs or affiliations, sexual orientation, health information, genetic information and has been extended to include biometric information.

APP 3.5 provides that an agency must collect personal information only by lawful and fair means.

APP 3.6 states that an agency must collect *personal information* about an individual only from an individual unless:

- the individual consents to the collection of the information from someone other than the individual;

- the entity is required or authorised under an Australian law, or a court/tribunal order, to collect the information from someone other than the individual; or
- it is unreasonable or impractical to do so.

12.2. APP 4 – Dealing with unsolicited personal information

Where an agency receives personal information which it did not ask for, the agency must, within a reasonable period of time, determine whether it could have collected the information lawfully under APP 3 (if the agency had sought the information).

APP 4.2 allows an agency to use or disclose the personal information for the limited purpose of making this determination.

If the agency determines that the personal information could have been collected lawfully then the rest of the APPs apply as if the information had been collected in that manner. On the other hand, if the agency determines that the information could not have been collected lawfully and the information is not contained in a Commonwealth record, it must destroy the information or de-identify it where it is otherwise lawful to do so.

12.3. APP 5 – Notification of collection of personal information

APP 5.1 provides that either at or before the collection of personal information, an agency must take reasonable steps to notify the individual, or otherwise ensure the individual is aware, of a number of matters set out at APP 5.2. If that timing is not practicable, the agency must do so as soon as practicable after the collection.

The relevant matters under APP 5.2 are:

- the agency's identity and contact details;
- if the agency collects personal information from a third party, or the individual may not be aware that the agency has collected their personal information, the fact the agency so collects, or has collected, the information and the circumstances of collection;
- the purposes for which the agency collects the personal information;
- the main consequences (if any) for the individual if all or some of the personal information is not collected by the agency;
- any other agency, body or person, to which the agency usually discloses personal information of the kind collected by the agency;
- that the agency's privacy policy contains information about how the individual may access the personal information about the individual that is held by the agency and seek the correction of such information;
- that the agency's privacy policy contains information about how the individual may complain about a breach of the APPs, or a registered APP code (if any) that binds the agency, and how the agency will deal with such a complaint;
- whether the agency is likely to disclose the personal information to overseas recipients; and
- if the agency is likely to disclose the personal information to overseas recipients, the countries in which such recipients are likely to be located if it is practicable to specify those countries in the notification or to otherwise make the individual aware of them.

13. DEALING WITH PERSONAL INFORMATION

13.1. APP 6 – Use or disclosure of personal information

APP 6.1 provides that if an agency holds personal information about an individual that was collected for the primary purpose, the agency must not use or disclose it for a secondary purpose unless:

- the individual has consented to the use or disclosure; or
- the use or disclosure of the information falls within the exceptions in APP 6.2.

APP 6.2(a) applies if the individual would reasonably expect the agency to use or disclose the personal information for the secondary purpose and the secondary purpose is related to the primary purpose. APP 6.2(b) permits the use or disclosure of personal information if it is required or authorised by or under an Australian law or a court/tribunal order.

13.2. APP 7 – Direct Marketing

APP 7 provides a regime for permitting use or disclosure of personal information for direct marketing purposes only if certain requirements are met. Generally speaking APP 7 will not apply to agencies. However, an agency can be treated as an organisation for the purposes of the APPs under section 7A of the Act.

13.3. APP 8 – Cross-border disclosure of personal information

Under APP 8.1, before an agency discloses personal information about an individual to an overseas recipient, it must take such steps as are reasonable in the circumstances to ensure that the overseas recipient does not breach the APPs in relation to the information.

However, APP 8.2 provides certain exceptions to the rule in APP 8.1. APP 8.2 states that APP 8.1 will not apply to cross-border disclosures of personal information in the following circumstances:

- where the agency reasonably believes that the overseas recipient of the information is subject to a law or binding scheme that has the effect of protecting the information in a substantially similar way in which the APPs protect the information, and there are mechanisms that the individuals can access to take action to enforce the law or binding scheme (Substantially Similar Law Exception); or
- where the individual consents to the disclosure after the agency expressly informs the individual that, if the individual consents to the disclosure of information, APP 8.1 will not apply to the disclosure (Informed Consent Exception).

APP 8.1 permits cross-border disclosure of personal information, ensuring that any personal information disclosed is still treated in accordance with the Privacy Act.

APP 8.1 and section 16C of the Privacy Act make an agency accountable for the personal information it collects and stores, even if that information is stored by a third party outside Australia. Indeed, section 16C deems the agency to be liable for acts and omissions of any overseas recipient to whom the agency has disclosed personal information that would breach the APPs.

13.4. APP 9 – Adoption, use or disclosure of government related identifiers

APP 9 generally prohibits the use or disclosure of a government related identifier. For the most part this will not be applicable to most agencies. However, an agency can be considered an organisation for the purposes of the APPs under section 7A of the Privacy Act.

14. INTEGRITY OF PERSONAL INFORMATION

14.1. APP 10 – Quality of personal information

Agencies are required to take reasonable steps to ensure that any personal information that is held by them is kept accurate, up-to-date, complete and relevant.

APP 10 imposes slightly different obligations in respect of the quality of personal information for information that is collected, as opposed to information that is used or disclosed:

- APP 10.1 requires agencies to take reasonable steps to ensure that any personal information collected is accurate, up-to-date and complete; and
- APP 10.2 requires agencies to take reasonable steps to ensure that personal information that it uses or discloses, having regard to the purpose of the use or disclosure, is accurate, up-to-date, complete and relevant.

14.2. APP 11 – Security of personal information

APP 11.1 requires agencies to take reasonable steps to protect personal information that they hold from misuse, interference, loss and unauthorised access, modification or disclosure.

Under APP 11.2, agencies must take reasonable steps to destroy or de-identify personal information if:

- the agency no longer needs the information for any purpose for which the information may be lawfully used or disclosed; or
- the information is not otherwise required to be kept under an Australian law or court order.

APP 11 applies to any personal information held by an agency, regardless of whether it collected that information.

15. ACCESS TO, AND CORRECTION OF, PERSONAL INFORMATION

15.1. APP 12 – Access to personal information

APP 12.1 requires agencies that hold personal information about an individual to give the individual access to that information on request by that individual, unless an exception applies.

APP 12.2 provides an exception to agencies in the event that the entity is required or authorised to refuse to give the individual access to the personal information under:

- the *Freedom of Information Act 1982* (Cth); or
- any other Act of the Commonwealth, or a Norfolk Island enactment, that provides for access by persons to documents.

APP 12.4 requires the agency to respond to requests for access to personal information within 30 days and to give access to the information in the manner requested by the individual, if reasonable and practicable to do so. Even if the agency refuses access on the basis of APP 12.2 or refuses to give access in the manner requested, APP 12.5 requires the agency to take reasonable steps to give access in a way that meets the needs of the agency and the individual. APP 12.6 specifically provides that access may be given through the use of a mutually agreed intermediary.

APP 12.7 provides that an agency cannot charge the individual for giving access to the personal information and cannot charge for the making of the request for access.

APP 12.9 provides that where an individual's request for personal information is refused, the individual must be given written reasons for the refusal unless it would be unreasonable to do so and the individual must also be advised of the mechanisms available to complain about the refusal.

15.2. APP 13 – Correction of personal information

An agency must take reasonable steps to ensure that personal information it collects and holds is correct.



APP 13.1 provides that an agency must take reasonable steps to correct personal information that it holds to ensure that, having regard to the purpose for which the information is held, it is accurate, up-to-date, complete, relevant and not misleading where:

- the agency is satisfied that the information is inaccurate, out-of-date, incomplete, irrelevant or misleading; or
- the individual whom the information is about requests the agency to correct the information.

Under APP 13.2, if an agency corrects an individual's personal information that it previously disclosed to another agency and the individual requests the entity to notify the other agency of the correction, the first agency must take reasonable steps to notify the other agency unless it is impracticable or unlawful to do so.

APP 13.3 provides that if an individual's amendment request is refused, the individual must be given written reasons for the refusal unless it would be unreasonable to do so. The individual must also be advised of the mechanisms available to complain about the refusal.

APP 13.4 provides that if an agency refuses to correct an individual's personal information as requested by the individual and the individual requests the entity to associate the information with a statement that the information is inaccurate, out-of-date, incomplete, irrelevant or misleading, the agency must take reasonable steps to associate the statement in a way that is apparent to users of the information.

APP 13.5 requires the agency to respond to requests under APP 13.1 or 13.4 within 30 days and to not charge for making the request, correcting the personal information or associating the statement with the personal information.