



Australian Government

Department of the Prime Minister and Cabinet

[Home](#) » [PM&C](#) » [Who We Are](#) » Privacy Policy

PRIVACY POLICY

OUR PRIVACY OBLIGATIONS

The Department has obligations for handling personal information as outlined in the:

- [Privacy Act 1988 \(Cth\)](#) (the Privacy Act), including the [Australian Privacy Principles \(APPs\)](#); and
- [Australian Government Agencies Privacy Code](#) (the Privacy Code).

The Department's Privacy Policy outlines what kinds of personal and sensitive information we collect, why we collect this information, and how we handle it.

'Personal information' means information or an opinion about an identified individual, or an individual who is reasonably identifiable.

'Sensitive information' is a subset of personal information and includes information or an opinion about an individual's:

- racial or ethnic origin
- political opinions
- religious beliefs or affiliations
- philosophical beliefs
- sexual orientation
- criminal record
- health information
- genetic information.

You can learn more about the Privacy Act and the Privacy Code on the [Office of the Australian Information Commissioner \(OAIC\)](#) website.

WHY WE COLLECT PERSONAL INFORMATION

We may collect personal information about you when it's reasonably necessary for, or directly related to, one or more of our functions or activities. We may collect sensitive information about

you where you consent, when the collection is authorised or required by law, or the collection is otherwise allowed under the Privacy Act. Find out more about our functions here: [who we are](#).

We collect, hold, use and disclose personal information for a range of purposes related to our functions and activities, including to:

- facilitate invitations for, and the running of, public submissions and consultations,
- seek feedback on policy, programs and services we deliver, and the review or reform of policy and processes,
- facilitate invitations to subscription services so that individuals who subscribe can receive information and other communications from the Department,
- undertake recruitment and maintain employment records,
- facilitate travel and security arrangements,
- conduct research we have commissioned or which we have partnered to deliver,
- coordinate on intergovernmental policy matters with States and Territories,
- respond to correspondence from members of the public or organisations to us, the Prime Minister, portfolio Ministers or other Australian Government Ministers and agencies,
- facilitate events, official visits, and appointments,
- administer honours and awards, deliver anniversary messages, and respond to requests for special access,
- process requests under the Freedom of Information Act 1982, and perform other legislative and administrative functions,
- handle complaints (including privacy complaints) and feedback provided to us,
- coordinate responses and provide crisis and recovery assistance in relation to an emergency or disaster, and
- administer programmes and grants.

HOW WE COLLECT PERSONAL INFORMATION

The Department may collect personal information about individuals in a variety of ways. This includes:

- from the individual directly, or through their authorised representative,
- via a third party if permitted by law.

Collection may be through surveys, email and phone communications, correspondence and submissions, forms and notices (including online portals), and via our websites.

HOW WE SAFEGUARD PERSONAL INFORMATION

The Department takes seriously its obligations to protect the personal information it holds. We take reasonable steps to protect your personal information against misuse, interference and loss,

and from unauthorised access, modification or disclosure. These steps include:

- classifying and storing records securely per Australian government security guidelines
- internal access to information is on a 'need to know' basis and only by authorised personnel
- monitoring system access with controls and authenticated credentials
- ensuring our buildings are secure
- regularly updating and auditing our storage and data security systems.

When personal information is collected from a third party, we take steps to inform of the collection. This may occur through this Privacy Policy, notices or discussions with our staff.

If personal information that we hold is lost, or subject to unauthorised access or disclosure, we will respond in line with the Office of the Australian Information Commissioner's [Data breach preparation and response —a guide to managing data breaches in accordance with the Privacy Act](#) and the Department's Data Breach Response Plan. We aim to provide timely advice to affected individuals if a data breach is likely to result in serious harm.

THE TYPES OF INFORMATION WE HOLD

In performing our functions, the Department may collect and hold the following kinds of personal and sensitive information:

- identity and contact details for individuals (e.g. name, phone, email and postal address),
- biometrics (such as photographs, video recordings and audio recordings of individuals),
- information relating to individuals' personal circumstances and health (e.g. age, gender, cultural and linguistic background, disabilities, medical history and other family circumstances including spouses, carers and dependents),
- information relating to individuals' financial affairs (e.g. payment details, bank account details),
- other information relating to identity (e.g. date of birth, citizenship and visa status, passport details, drivers licence, racial and ethnic origin),
- information about political or union memberships and associations,
- information about criminal activities individuals may have been involved in,
- information about employment (e.g. employment status and work history, education status, referee comments, salary), and
- government identifiers (e.g. tax file number).

We may also collect information about how you use our online services and applications. For example, we use social networking services such as Facebook, Twitter and LinkedIn to talk with the public and our staff. When you talk with us using these services we may collect your personal information to communicate with you and the public. These social networking services will also handle your personal information for their own purposes. These services have their own privacy policies. You can access the privacy policies for these services on their websites.

HOW WE USE AND DISCLOSE INFORMATION

The Department may use and disclose collected personal information for the primary purpose of collection, and where we are otherwise permitted by law to use and disclose it. We will take reasonable steps to give you information about the reason for collection at the time of collection, or as soon as practicable thereafter. The Department will only use and disclose your personal information for a secondary purpose if APP 6 allows it.

We may disclose personal information to overseas entities (such as a foreign government or agency) where this is a necessary part of our work. We will only do this with your consent or in other circumstances allowed by APP 8.

We may also use third party providers such as Google, Facebook, Twitter, Campaign Monitor, LinkedIn, Qualtrics, Instagram, YouTube and others to deliver or otherwise communicate content. Such third-party sites have their own privacy policies and may send their own cookies to your computer. We do not control the setting of third-party cookies and suggest you check the third-party websites for more information about their cookies and how to manage them.

WEBSITE ANALYTICS

To improve your experience on our site, we may use 'cookies'. Our website also uses Google Analytics, a service which transmits website traffic data to Google servers in the United States. Google Analytics does not identify individual users or associate your IP address with any other data held by Google. We use reports provided by Google Analytics to help us understand website traffic and webpage usage – to improve your interactions with us.

By using this website, you consent to the processing of data about you by Google in the manner described in [Google's Privacy Policy](#) and for the purposes set out above. You can opt out of Google Analytics if you disable or refuse the cookie, disable JavaScript, or [use the opt-out service provided by Google](#). Our website may also contain links to other websites. Please be aware that we are not responsible for the privacy practices of such other sites. When you go to other website from here, we advise you to be aware and read the respective privacy policies.

Find out more about the Department's collection and use of information from our websites and social media platforms in our [Website and Online Communications Privacy Collection Notice](#).

ACCESSING AND CORRECTING PERSONAL INFORMATION

You have a right to request access to personal information we hold about you, and to request its correction. We will respond to requests for access or correction within 30 days.

The Privacy Act allows us to refuse access in certain cases, including where an exemption under the *Freedom of Information Act 1982* (FOI Act) would apply. Where we have refused access, we will give you reasons in writing. We will also provide you with information about how you can dispute the decision.

To request access to, or correction of, your personal information please contact our Privacy Officer. Discussing your request with our Privacy Officer will help us give you early guidance about your request. This may include guidance about whether your request is best dealt with under the Privacy Act, the FOI Act or another arrangement.

PRIVACY IMPACT ASSESSMENTS

The Privacy Code requires agencies, including the Department, to conduct a Privacy Impact Assessment (PIA) for all high privacy risk projects.

PIAs completed by the Department, since the Privacy Code commenced on 1 July 2018, are listed in the table below.

Date	Title
October 2021	Updated Final PIA on the case management system – independent complaints and support service for serious incidents
August 2021	Draft PIA on the case management system – independent complaints and support service for serious incidents
8 March 2021	PIA on the <i>Data Availability and Transparency Bill 2020</i>
17 February 2021	Joint PIA with the National Drought and North Queensland Flood Response and Recovery Agency (NDFA) on proposed Client Relationship Management system
6 September 2020	Draft PIA on the <i>Exposure Draft Data Availability and Transparency Bill 2020</i>
28 June 2019	PIA on the <i>Proposed Data Sharing and Release (D&R) Bill and Related Regulatory Framework</i>

HOW TO MAKE A PRIVACY COMPLAINT

If you are not satisfied with how we have collected, held, used or disclosed your personal information, you can make a formal complaint to our [Privacy Officer](#).

Your complaint should include:

- A short description of your privacy concern,
- Any action or dealings you have had with staff of the Department to address your concern; and
- Your preferred contact details so we can contact you about your complaint.

If we do not resolve your privacy complaint to your satisfaction, you may lodge a complaint with the Office of the Australian Information Commissioner (OAIC).

The OAIC can receive privacy complaints through:

- the online Privacy Complaint form (refer to the [OAIC's website](#))
- by email (email that is not encrypted can be copied or tracked) at enquiries@oaic.gov.au
- by mail (if you have concerns about postal security, consider sending your complaint by registered mail)
- Office of the Australian Information Commissioner
Sydney Offices
GPO Box 5218
Sydney NSW 2001
- by fax at +61 2 9284 9666

HOW TO CONTACT OUR PRIVACY OFFICER

Contact the Department's Privacy Officer if you want to:

- Ask questions about our Privacy Policy, or if you need a copy of this Policy in an alternative format;
- Obtain access to or seek correction of your personal information held by the Department; or
- Make a privacy complaint about the Department.

Email: privacy@pmc.gov.au

Post: The Privacy Officer

Department of the Prime Minister and Cabinet

PO Box 6500

CANBERRA ACT 2600

We review this Policy regularly, and may update it from time to time.

This Policy was last updated on: 28 April 2021



Australian Government

Department of the Prime Minister and Cabinet

Privacy Management Plan


Supporting privacy success at PM&C

1 August 2021

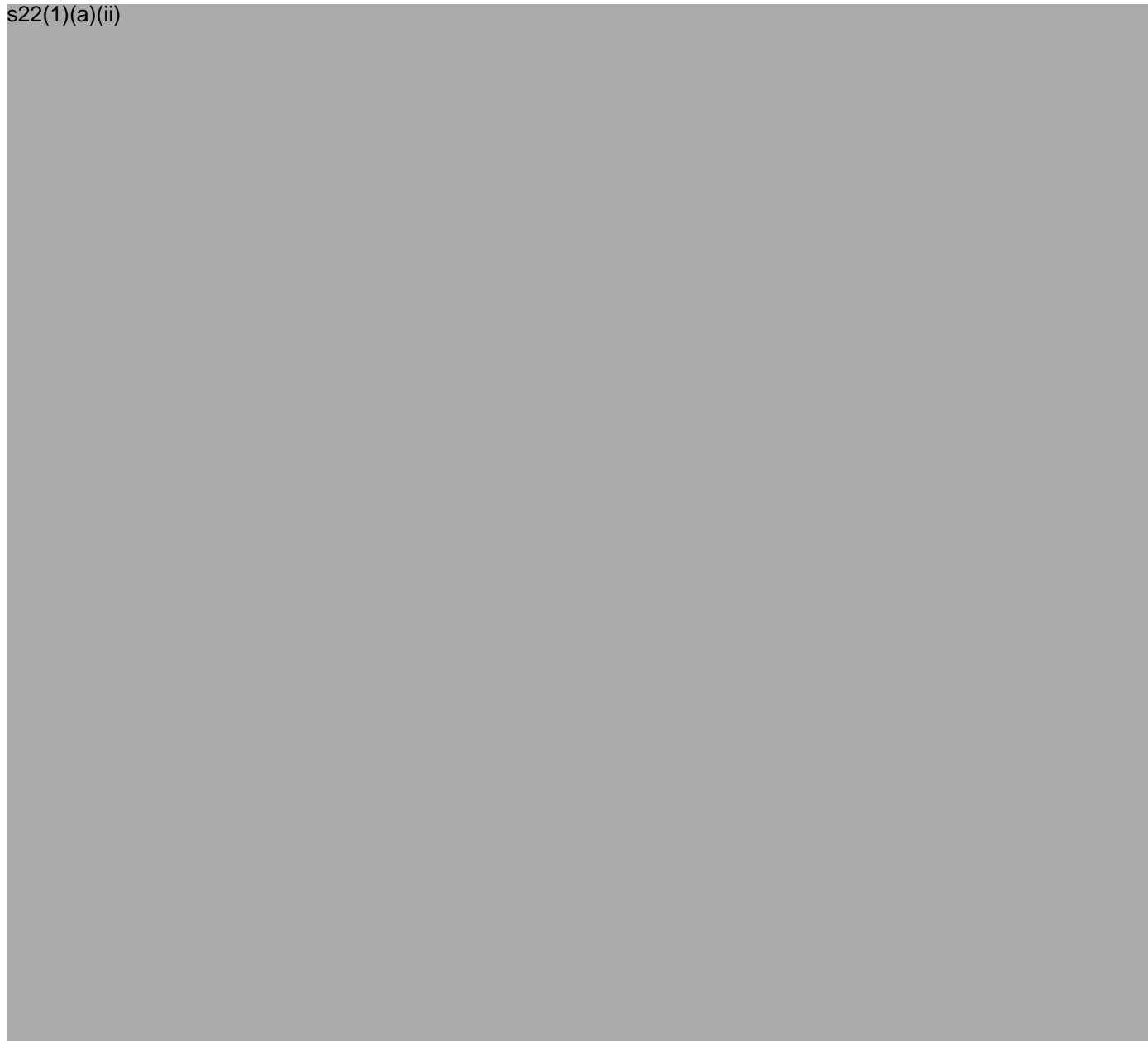
Table of Contents

Table of Contents	1
Executive Summary	2
Overview	2
Purpose	2
Background.....	2
Managing Privacy within the Department	3
The Department's privacy obligations	3
Privacy Deliverables and Priorities	4
Measuring Performance and Privacy Maturity – Annual Review.....	4
The OAIC Maturity Framework	4
The Department's Privacy Maturity Benchmark	5
Attachments:	6
A. PMP Compliance Deliverables and Actions	6
B. The Australian Privacy Principles (APPs)	13
C. The Privacy Code – Key Obligations.....	15
D. Key Definitions: Personal and Sensitive Information.....	16

s22(1)(a)(ii)



s22(1)(a)(ii)

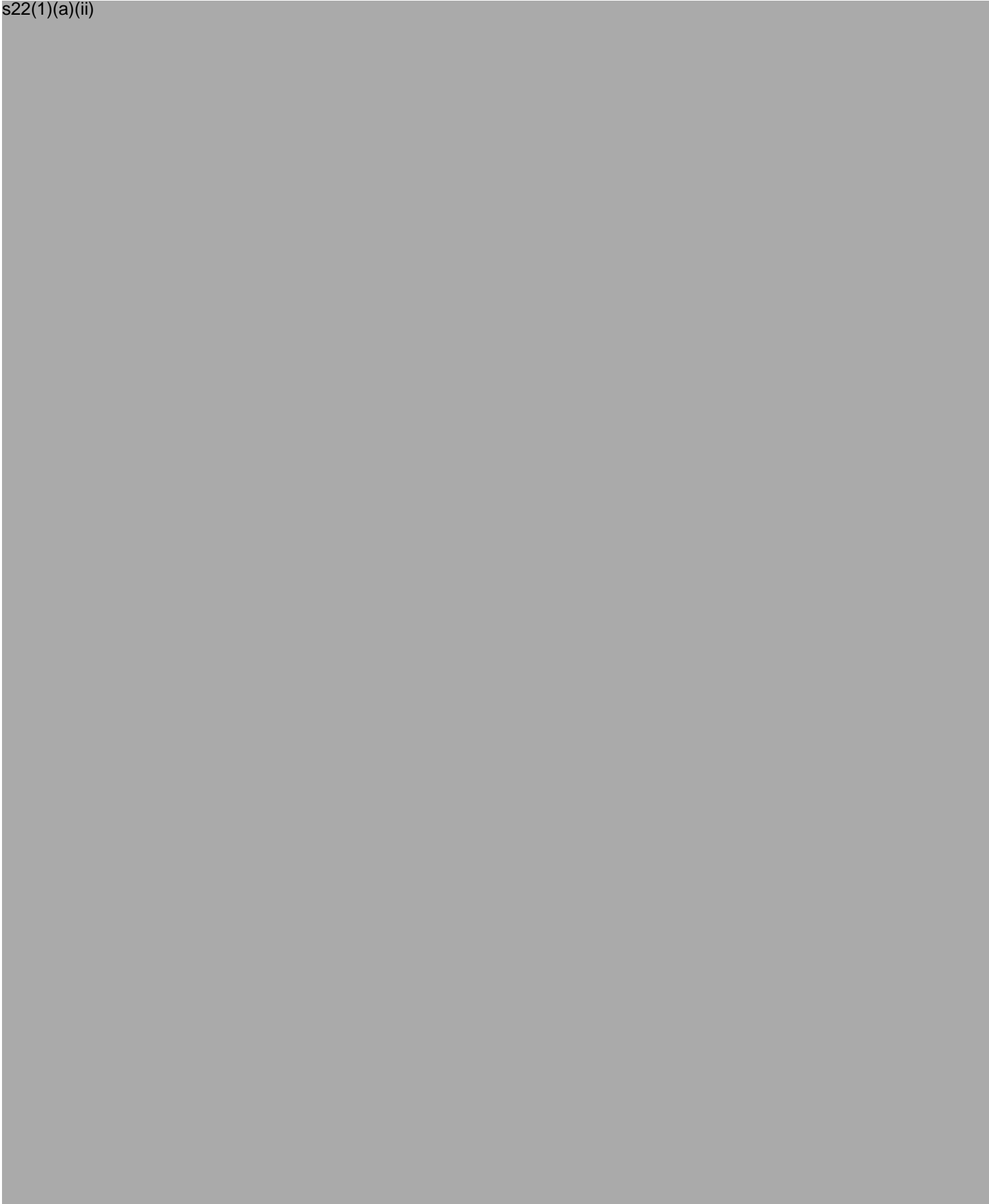


Section 15 of the Privacy Act provides that an APP entity, such as the Department, must not do an act, or engage in a practice, that breaches an APP. An act or practice that breaches an APP or a binding Code is an ‘interference with privacy’.

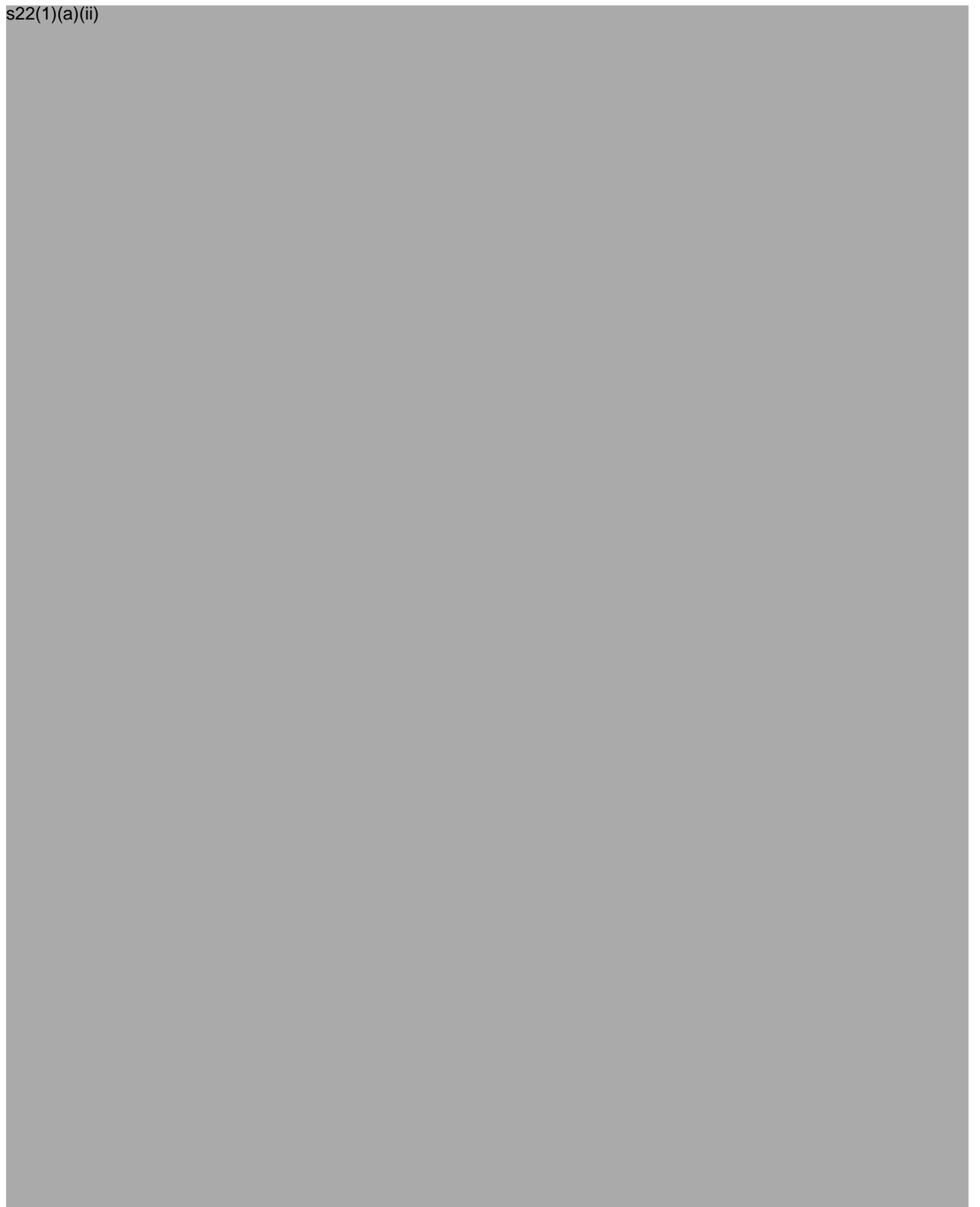
An individual can complain to the Privacy Commissioner about an interference with privacy and the Commissioner can also conduct “own motion” audits. If the Commissioner finds there has been an interference with privacy, the Commissioner can make certain determinations including that an agency take remedial action or pay compensation (section 52, Privacy Act).

Under APP 1.2, the Department is required to take reasonable steps to implement practices, procedures and systems that ensure compliance with the APPs and the Privacy Code.


s22(1)(a)(ii)




s22(1)(a)(ii)




s22(1)(a)(ii)




s22(1)(a)(ii)




s22(1)(a)(ii)




s22(1)(a)(ii)




s22(1)(a)(ii)



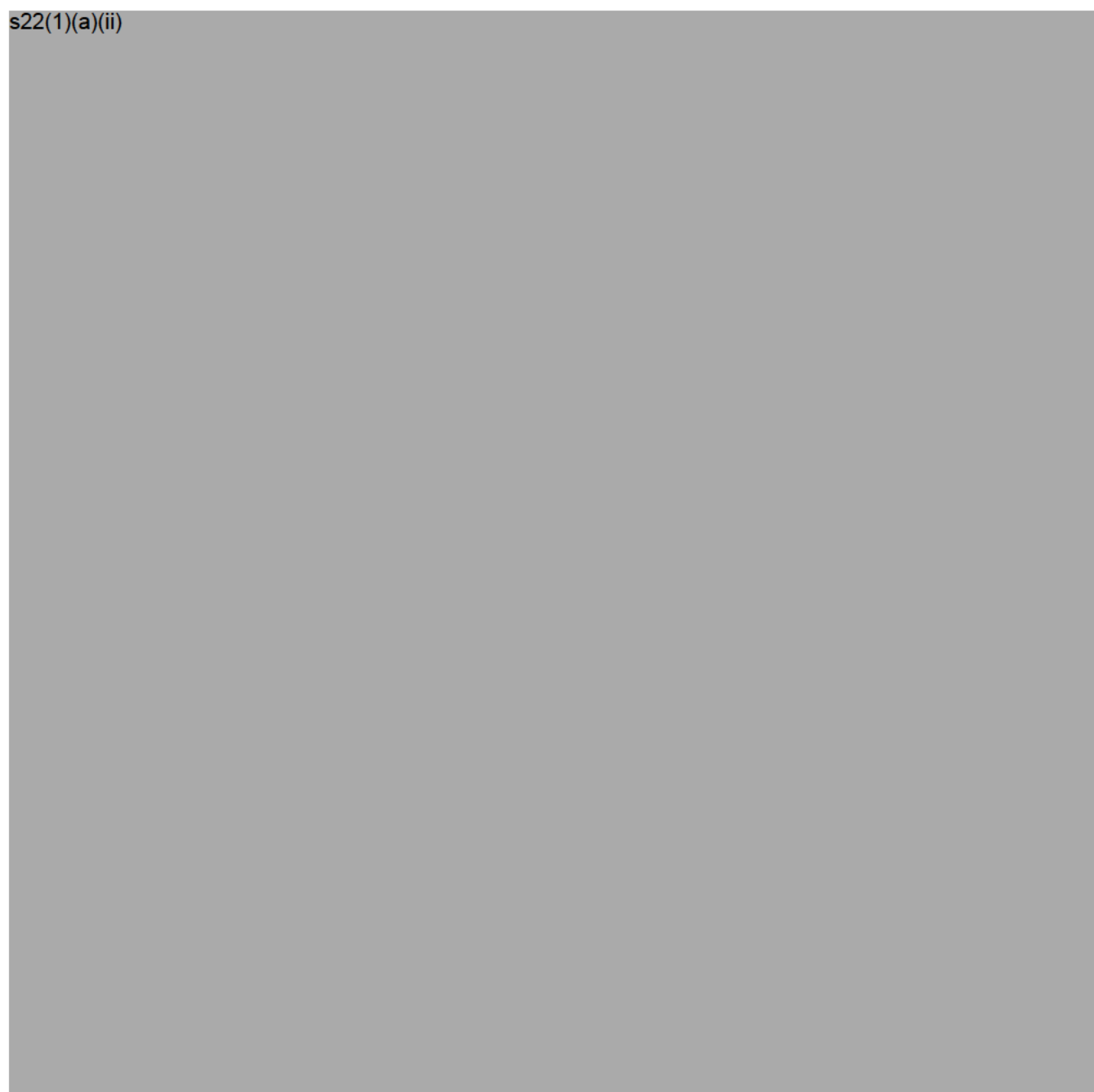
s22(1)(a)(ii)



s22(1)(a)(ii)



s22(1)(a)(ii)




individual consented, or the purpose is related and the individual would expect the use or disclosure.

Exceptions to the general rule: if it is for secondary purpose, the use or disclosure will be permitted in prescribed

s22(1)(a)(ii)

s22(1)(a)(ii)



D. Key Definitions: Personal and Sensitive Information

Personal information

The Privacy Act regulates the collection, storage, use, correction and disclosure of ‘personal information’.

Determining whether or not particular information is ‘personal information’ is a critical threshold question for whether the APPs apply. For any project a key question is whether it is truly necessary to collect identifying information to achieve a project purpose and, if it is, what identifying information is actually needed for that purpose (see in particular APP 3).

“Personal information” is defined as:

"information or an opinion about an identified individual, or an individual who is reasonably identifiable:

- (a) whether the information or opinion is true or not; and
- (b) whether the information or opinion is recorded in a material form or not”.

(s.6 Privacy Act)

Compliance risk can be reduced by taking steps (if possible and practicable) to de-identify information such that it no longer has the character of being personal information.

Sensitive information

Most ‘sensitive information’ can be described as a special subset of ‘personal information’.

APPs 3.3, 3.4, 6.2, 7.4 set out specific rules for handling sensitive information. Generally, for an APP agency to collect sensitive information, the information must be reasonably necessary for, or directly related to, one or more functions and the individual consents to collection.

“Sensitive information” is defined as:

- (a) information or an opinion about an individual’s:
 - (i) racial or ethnic origin; or
 - (ii) political opinions; or
 - (iii) membership of a political association; or
 - (iv) religious beliefs or affiliations; or
 - (v) philosophical beliefs; or
 - (vi) membership of a professional or trade association; or
 - (vii) membership of a trade union; or
 - (viii) sexual orientation or practices; or
 - (ix) criminal record;
 that is also personal information; or
- (b) health information about an individual; or
- (c) genetic information about an individual that is not otherwise health information; or
- (d) biometric information that is to be used for the purpose of automated biometric verification or biometric identification; or
- (e) biometric templates.



TEMPLATE PRIVACY NOTICE

Purpose

A Privacy Notice is a legal requirement under [Australian Privacy Principle \(APP\) 5](#) of the [Privacy Act 1988](#) (Privacy Act). A Privacy Notice tells people:

- what personal information the Department is collecting at that point in time,
- why the Department is collecting the personal information,
- whether people have a choice to provide the information, and
- how the Department will use and disclose the information.

This template Privacy Notice is designed to meet the requirements of the Privacy Act; however, it is a guide only and should be customised to suit the circumstances in which information is being collected.

Further guidance about Privacy Notices is available from the Office of the Australian Information Commissioner [here](#).

Contact the Privacy Officer at privacy@pmc.gov.au or on x5974 if you have any questions about using the template.

Instructions on how to use the template

- Adapt as appropriate
- Insert the Privacy Notice at an appropriate point on the website or other notification format **before** users are required to upload or provide personal information.
- Consent may be required to collect certain types of personal information; such as health information and other **sensitive** information (as defined in section 6 of the Privacy Act), or when disclosing personal information overseas.
 - Contact the Privacy Officer if you need advice about consent – consent is a separate process from a Privacy Notice.
- Please send a copy of your draft Privacy Notice to the Privacy Officer at privacy@pmc.gov.au for review and settling.

PRIVACY NOTICE TEMPLATE

The Department of the Prime Minister and Cabinet (the Department) is collecting your personal information to *<describe the primary purpose/s of collection, eg process your application; inform the Government's consultation about X; provide you information and updates on X etc >*

For the same purpose/s, we may provide this information to *<list the people, agencies or organisations outside the Department to whom we will routinely disclose the personal information, eg agency X including Ministers, an events organiser, other service provider or third party contractor>*

We may also disclose your personal information to overseas recipients *<specify the countries in which recipients are located if practicable or delete if not applicable>*.

Providing the requested information is *<insert 'voluntary' or 'required by law' (specify which law if practicable)>*. If you choose not to provide us with your information *<describe the main consequence, eg we will be unable to assess your application, or provide you with X service>*.

The Department will not provide the information collected from you to anyone else outside the Department *[other than to X, above]* unless you have given consent for us to do this, or we are authorised or required to do so by law.

The privacy and security of your personal information is important to us, and is protected by law. The Department's [Privacy Policy](#) explains how the Department handles and protects the information provided by you. Our Privacy Policy also explains how you can request access to or correct the personal information we hold about you, and who to contact if you have a privacy enquiry or complaint. If you require a copy of our Privacy Policy contact the Privacy Officer at privacy@pmc.gov.au