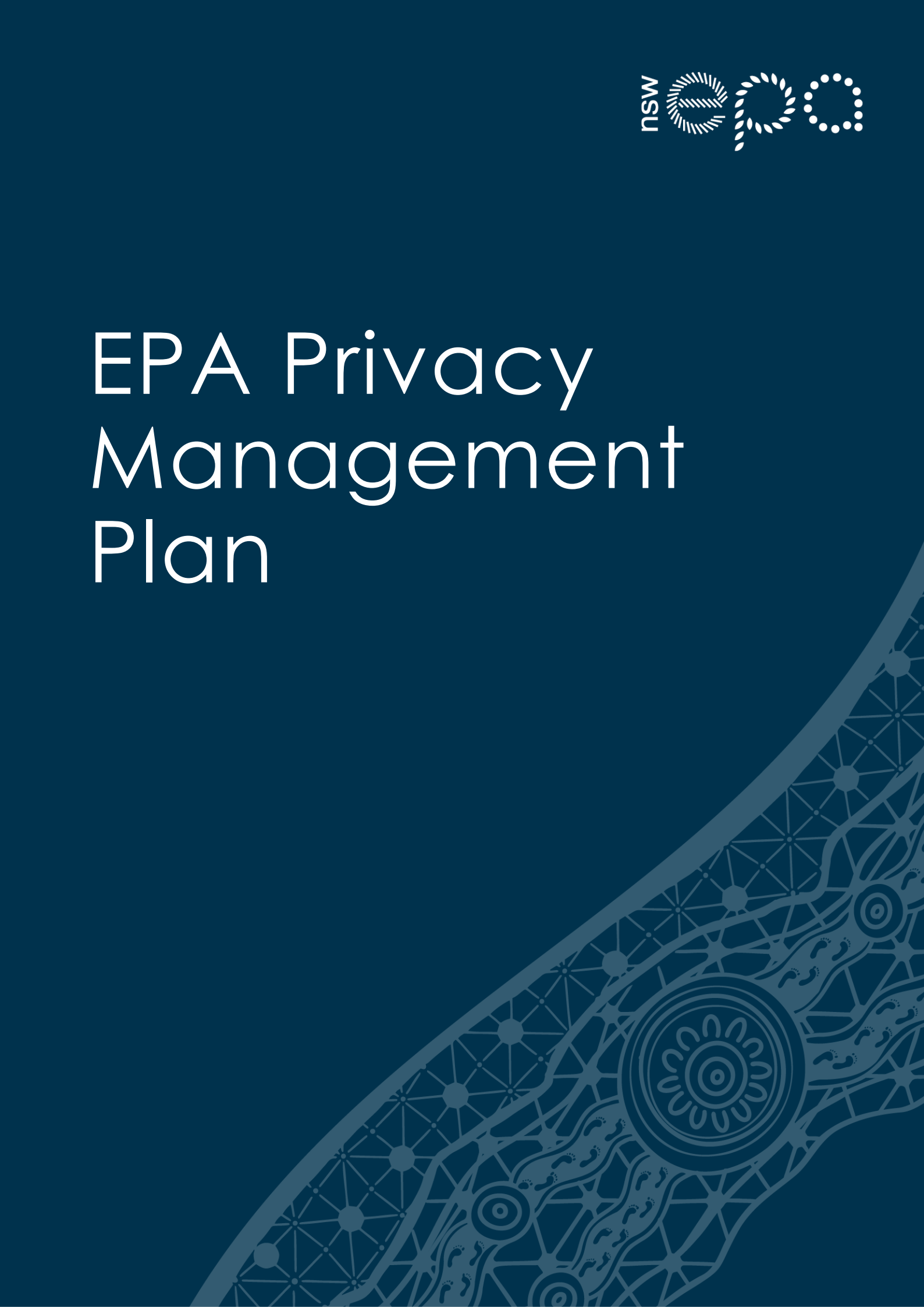
EPA Privacy Management Plan



Acknowledgement of Country

The NSW Environment Protection Authority acknowledges the Traditional Custodians of the land on which we live and work, honours the ancestors and the Elders both past and present and extends that respect to all Aboriginal people.

We recognise Aboriginal peoples' spiritual and cultural connection and inherent right to protect the land, waters, skies and natural resources of NSW. This connection goes deep and has since the Dreaming.

We also acknowledge our Aboriginal and Torres Strait Islander employees who are an integral part of our diverse workforce and recognise the knowledge embedded forever in Aboriginal and Torres Strait Islander custodianship of Country and culture.

Published by:
NSW Environment Protection Authority

6&8 Parramatta Square
10 Darcy Street,
Parramatta NSW 2150
Locked Bag 5022,
Parramatta NSW 2124

Phone: +61 2 9995 5000 (switchboard)
Phone: 131 555
(NSW only – environment information and publications requests)

Fax: +61 2 9995 5999

TTY users: phone 133 677,
then ask for 131 555

Speak and listen users:
phone 1300 555 727,
then ask for 131 555

Email: info@epa.nsw.gov.au
Website: www.epa.nsw.gov.au

Report pollution and environmental incidents
Environment Line: 131 555 (NSW only) or info@epa.nsw.gov.au
See also www.epa.nsw.gov.au

ISBN 978 1 922963 86 4
EPA 2024P4528
June 2024

Contents

1. Introduction

The *Privacy and Personal Information Protection Act 1998* (PPIP Act) and the *Health Records and Information Privacy Act 2002* (HRIP Act) contain principles on how public sector agencies must manage personal and health information. They also require the Environment Protection Authority (EPA), as a public sector agency, to prepare and implement a privacy management plan.

This privacy management plan (the plan) identifies the measures the EPA takes to comply with the PPIP Act and the HRIP Act.

This plan has been prepared and implemented as required under section 33 of the PPIP Act, and includes:

- the EPA's policies and practices to ensure compliance with the PPIP Act and the HRIP Act
- how the EPA circulates those policies and practices within the EPA
- the procedures the EPA provides for internal review under Part 5 of the PPIP Act
- matters the EPA considers relevant to privacy and the personal and health information it holds.

The plan also describes how individuals can request access to and amend their personal or health information held by the EPA.

2. Plan

2.1. Objectives

The objectives of this plan are to detail how:

- the EPA protects the privacy of our stakeholders, employees and others about whom we hold information
- EPA employees should manage and protect personal/health information
- individuals can ask to access, amend or suppress their personal/health information held by the EPA
- the EPA integrates the Information Protection Principles and Health Privacy Principles into our policies, guidelines and procedures concerning information management
- the EPA manages privacy complaints and internal reviews
- individuals can ask for an internal review
- individuals can apply to the NSW Civil and Administrative Tribunal (NCAT) if they are dissatisfied with internal review findings.

2.2. EPA policies and practices

The EPA employs the following broad strategies to ensure ongoing compliance with privacy legislation:

- as part of our induction program, new staff are provided with information to raise their awareness and appreciation of the privacy legislation requirements
- the Privacy Management Plan is promoted during the annual Privacy Awareness Week
- the Risk and Governance team provides advice internally to staff, relating to the interpretation and practical implementation of the privacy legislation
- the plan is published on our intranet and website
- the plan is reviewed and updated every three years.

2.3. Scope

This plan applies to all EPA employees including ongoing, term, temporary, casual and seconded employees

This plan applies to contractors who are representing the EPA or third-party contractors, including volunteers, agents, contingent workers, labour hire, independent contractors and consultants who may have access to personal or health information held by the EPA in the course of their engagement with the EPA.

This plan does not apply to contractors who are not representing the EPA but are providing professional services to the EPA and do not have access to personal information held by the EPA in the course of their engagement with the EPA.

2.4. Non-compliance with the plan, and criminal offences

Non-compliance with this plan by EPA employees will be managed in accordance with the EPA's *Managing Misconduct Policy* (2022) and section 69 of the *Government Sector Employment Act 2013.*

All employees, volunteers and third-party contractors included in the Scope at 2.2 above are required to comply with the PPIP Act and the HRIP Act. Both Acts contain criminal offence provisions applicable to employees and contractors who use or disclose personal or health information without authority.

It is an offence to:

- intentionally disclose or use for an unauthorised purpose personal or health information accessed
- offer to supply personal or health information for an unauthorised purpose
- attempt, by threat, intimidation, etc., to dissuade a person from making or pursuing a request for health information, a complaint to the NSW Privacy commissioner about health information, or an internal review under the HRIP Act, or
- hinder the Privacy Commissioner or member of staff from exercising their official functions.

It is a criminal offence, punishable by up to two years' imprisonment, an $11,000 fine, or both, for any person employed or engaged by the EPA (including former employees and contractors) to intentionally use or disclose any personal information or health information about another person, to which the employee or contractor has or had access in the exercise of their official functions, except in connection with the lawful exercise of their official functions.

It is also an offence to access or modify computer records for purposes not connected with the duties of the person.

Employees who are uncertain whether certain conduct may breach their privacy obligations should seek advice from the relevant team. See *Appendix A1.3: Advice*.

3. Information collected by the EPA

3.1. EPA functions

The EPA is a statutory corporation established under section 5 of the *Protection of the Environment Administration Act 1991*.

Information held by the EPA will be used for the intended purpose only, in keeping with the EPA's functions, records management and other policies, agreements and this plan.

Some of the functions of the EPA include:

- consultation and engagement with the community, industry and other stakeholders
- investigation of pollution incident reports, potential breaches of legislation/policies and other allegations
- site audits and inspections, and incident management and enforcement of environmental regulations
- issuing licences, approvals, consents and permits.

3.2. Types of information/documents collected

The EPA holds document types that include personal and privacy related information. These fall within the following major categories:

- personnel records and files
- incident reports, application forms for licences and permits
- complaints and reports of environmental and pollution incidents
- reports of investigations (e.g. research, audits, ethical conduct, compliance)
- public registers, public submissions, feedback and comments
- databases containing personal information
- financial transactions for payment of goods and services delivered by or to the EPA
- fines issued
- information agreements and other agreements
- mailing lists and subscriptions to publications or email alerts or notifications
- verbal/photographic/audio/video records.

There are also health and personal records:

- relating to levels of exposure to radiation of certain employees and health practitioners
- concerning most employees, such as details about payroll, leave, training, workers compensation, vaccinations, medical certificates and similar/other personnel records.

3.3. Requests regarding personal information

The EPA collects personal information about people. Individuals can request:

- access to their personal information (see details in section 5.3)
- amendments to their personal information (see details in section 5.5)
- suppression of their personal information (see details in section 7.1).

Contact the Risk and Governance team to request access, amendment or suppression. See *Appendix A1.3: Advice*.

3.4. Mitigating the risk of identity fraud

When sending personal information by post, email or social media, the EPA needs to mitigate the risk of someone intercepting the correspondence and using the personal details in the document for identity fraud.

To reduce this risk, the EPA keeps personal information in any correspondence (including attachments) to a minimum.

For information made digitally available, the EPA de-identifies, anonymises or redacts it, to remove personal identifying information.

3.5. Sharing information: Data Analytics Centre and other agencies

The *Data Sharing (Government Sector) Act 2015* (DSGS Act) promotes sharing of information for certain purposes. This includes carrying out data analytics to identify issues and solutions, to develop government policy, program management, and service planning and delivery.

The DSGS Act provides for the expeditious sharing of information with the Data Analytics Centre and other public sector agencies. It also provides protections in connection with data sharing and ensures compliance with the requirements of the PPIP Act and the HRIP Act.

The EPA is required to ensure:

- health and/or personal information in the shared data environment complies with privacy legislation
- any confidential and commercial-in-confidence information in the shared data environment complies with any contractual or equitable obligations of the data provider.

Before responding to a request from Data.NSW to provide information, the EPA consults internally with the Risk and Governance team to obtain relevant advice (see *Appendix A1.3: Advice*). The EPA may also ask the Privacy Commissioner to guide it on the best way to comply with the request for information while upholding the IPPs and HPPs.

If the EPA receives a request from another public sector agency, before releasing information to the other agency, the EPA must check the named legislation relied upon for the provision of information, and ensure that the request is legitimate.

If in doubt about the legitimacy of the request, the EPA checks internally with its Risk and Governance team, seeks legal advice, or contacts the agency requesting the information.

3.6. Transborder flows of personal information

Section 19(2) of the PPIP Act provides additional requirements for disclosing information outside NSW. If information needs to be disclosed to a recipient outside the NSW jurisdiction or to a Commonwealth agency, there are some additional criteria to be met. These are set out in the Guidance: Transborder Disclosure Principle provided by the Office of the Privacy Commissioner.

Before any personal information is disclosed outside NSW, the EPA makes enquiries to ensure the intended recipient has similar privacy laws.

The EPA may draw up an agreement that meets the requirements of section 19(2) of the PPIP Act and/or seek legal advice.

In July 2021, the Commonwealth, all states and both territories entered an intergovernmental agreement to share data across jurisdictions, where it can be done securely, safely, lawfully and ethically.

The *Data Availability and Transparency Act 2022* (Clth) establishes a legislative scheme for sharing public sector data with Commonwealth, state and territory bodies and Australian universities.

3.7. Workplace surveillance

Where EPA work locations have cameras, computers or tracking devices to carry out surveillance of their employees, the EPA must comply with the *Workplace Surveillance Act 2005.*

Members of the public are not affected by this, other than perhaps by being captured by the video recordings, tracking or other surveillance in place.

In general, employers may carry out a wide range of surveillance, if employees are properly notified and aware of it. This is called 'overt surveillance'.

Surveillance where employers do not properly notify employees is generally prohibited by legislation except for the purposes of establishing whether employees are involved in unlawful activity while at work.

This is called 'covert surveillance'. Covert surveillance needs the authority of a magistrate.

Recording of private conversations is covered by the *Surveillance Devices Act 2007*. Legal advice should be sought in respect of both workplace surveillance and the recording of private conversations.

Overt surveillance

For overt surveillance, employees must be given written notice that includes the following items:

- the **kind** of surveillance used (e.g. camera, computer, or tracking)
- **how** the surveillance will be carried out
- **when** it will start
- if it will be **continuous** or **intermittent**, and
- if the surveillance will be **ongoing** or for a specified **limited period**.

Information gained from overt surveillance cannot be used or disclosed unless the use or disclosure is:

- related to the employment of EPA employees
- related to EPA business activities or functions
- given to a law enforcement agency in relation to an offence
- related to civil or criminal proceedings, or
- reasonably believed necessary to avert an imminent threat of serious violence to persons or substantial damage to property.

Breaching the above restrictions carries a fine.

Access to the information can be requested by an employee or a person who was captured by the surveillance. Such requests can be made under the PPIP Act or the *Government Information (Public Access) Act 2009*.

4. Risk management

4.1. Privacy impact assessment

A privacy impact assessment (PIA) may be used to assess any actual or potential effects that an activity, project or proposal may have on personal information held by the EPA. A PIA can also outline ways in which any identified risks could be mitigated, and any positive impacts enhanced.

A PIA is a systematic assessment that identifies the impact a project may have on the privacy of individuals. It sets out recommendations for managing, minimising or eliminating that impact.

Public consultation and measuring community expectations are important parts of any thorough PIA. A PIA should examine both the positive (privacy-enhancing) and negative (privacy-invasive) impacts.

Privacy risks can be avoided or mitigated by:

- ensuring a project complies with the law
- ensuring a project meets community expectations
- making a project less privacy-invasive
- making a project more privacy-enhancing.

Not all risks can be eliminated every time; however, judgements have to be made as to whether the public benefit outweighs the risk posed to privacy.

A PIA helps to:

- diagnose risks, benefits, costs and safeguards involved
- ensure compliance with privacy legislation
- reduce costs in management time, legal expenses, and potential media or public concern, by considering privacy issues early
- anticipate and respond to possible privacy concerns
- enhance informed decision-making
- enhance the legitimacy of a project, especially where a compromise or trade-off is necessary.

To work out whether a PIA should be considered, complete the privacy impact assessment checklist. If the answer to one or more of the questions is “Yes”, then a privacy impact assessment (PIA) should be considered.

4.2. Privacy impact assessment checklist

No.	Will the project involve:	Yes	No
1.	The collection of personal information, compulsorily or otherwise?		
2.	A new use of personal information that is already held?		
3.	A new or changed system of regular disclosure of personal information, whether to another agency, another state, the private sector, or the public at large?		
4.	Restricting access by individuals to their own personal information?		
5.	New or changed confidentiality provisions relating to personal information?		
6.	A new or amended requirement to store, secure or retain personal information?		
7.	A new requirement to sight, collect or use existing ID, such as an individual’s driver’s licence?		
8.	The creation of a new identification system, e.g. using a number or a biometric?		

9.	Linking or matching personal information across or within agencies?
10.	Exchanging or transferring personal information outside NSW?
11.	Handling personal information for research or statistics, de-identified or otherwise?
12.	Powers of entry, search or seize, or other reasons to touch another individual e.g. taking a blood or saliva sample?
13.	Surveillance, tracking or monitoring of individuals' movements, behaviour or communications?
14.	Moving or altering premises which include private spaces?
15.	Any other measures that may affect privacy?

If the outcome is that:

- a PIA should be conducted, contact the Risk and Governance team. (See Appendix A1.3, *Advice*.)
- a PIA is not needed, make a note and copy of the above questions and save to file. Email your note to EPA CSB GIPA Privacy Mailbox. This helps if privacy issues arise later and you need to re-visit the list.

It is not compulsory to have a PIA, but it is recommended. Even if the list above does not indicate the need for a PIA, it may still be advisable to create a short PIA, particularly if the project will change hands several times. A consistent approach to the management of privacy in a project is crucial.

A PIA should contain some or all the following 10 steps.

Step	Action	Consider the following
1.	Assess if a PIA is required	Use the PIA checklist in this document.
2.	Plan the PIA. How detailed does it need to be?	• Will it cover one product and service or a group of products and services? • Identify the primary stakeholders. • Scope the complexity of the product and service. • Will there be community or media interest in the outcome?
3.	Describe the project (briefly)	• What are the project's overall aims? • Who is responsible? • What is the time frame?
4.	Identify the stakeholders	• Who are the stakeholders? • Are consultations required to discuss potential risks and concerns?
5.	Map information flows…	• Map the data life cycle. • What is collected, how, by whom, and where is it going? • Where will this information be stored? • What are the security and quality processes around the data? • Map the data against compliance with the IPPs and HPPs and identify gaps..
6.	Privacy impact analysis and compliance check…	• After *Step 5: Map information flows*, analyse the identified gaps • Identify the risks and their sources. • identify the data or compliance leakage.
7.	Address privacy management risks…	• What options allow you to remove, minimise or mitigate any identified risks? • Is collection of personal data necessary? • Are you being transparent enough (privacy notice issued)?

Step	Action	Consider the following
8.	Formulate recommendations for future projects…	• Are there any changes that would achieve a more appropriate balance between the project's goals, the interests of affected individuals, and the agency's interests? • Are any of the identified privacy impacts so significant that the project should not proceed?
9.	Prepare the report to include…	• An overall description • Your PIA method • Description of the data flows • Outcome of the PIA and compliance checks • How to mitigate and avoid risks in future • Identification of the community's response to these risks.
10.	After the PIA report…	• Have you responded to the recommendations in the PIA report? • Have you engaged an independent review of these recommendations? • Has the PIA changed due to any changes in the project?

4.3. Seeking consent

The EPA is obliged to provide a notification or privacy statement when personal information is collected. If the information is to be used for another purpose than the purpose for which it was collected, consent **must** be specifically sought. Individuals must be adequately informed before giving consent. Consent means 'express consent or implied consent' and should:

- be provided voluntarily i.e. the individuals had the opportunity to provide or withhold consent without any coercion or duress to overpower the individuals' will
- be current and specific
- consider the individuals' capacity to understand and communicate their consent.

Template privacy notifications/statements can be found at *Procedure 3: Privacy notices and consent*.

5. Application of the Information Protection Principles (IPPs)

The twelve Information Protection Principles (IPPs) from the PPIP Act establish the legal obligations and standards for collecting and dealing with personal information to minimise the risk of its misuse.

The degree of sensitivity of the personal information influences the way in which the IPPs are applied. The more sensitive the nature of the information, the higher the level of care that needs to be used when dealing with the information, particularly where disclosure to a third party is being considered.

The key stages in the personal information management cycle are:

- collection
- storage
- access
- amendment
- use
- disclosure
- destruction (when the data is no longer needed for the purpose for which it was collected).

5.1. Collecting personal information (IPPs 1–4)

The EPA only collects personal information for a lawful purpose directly related to, and reasonably necessary for, its work. Generally, the EPA collects personal information directly from individuals, unless they have authorised someone else to provide it or if the parent or guardian of an individual aged under 16 years has provided it.

Some exceptions are in place to authorise public sector agencies to collect information from another public sector agency: see *8: Exemptions under the PPIP Act*. Individuals whose personal information was collected when they were minors may have a right to access, modify and supress their personal information once they are over 16 years.

Below are possible ways of collecting personal information; however, the EPA may not use all of them.

1. **Provided** by individuals through direct actions of which they are aware e.g.:
   a. registering on the EPA website
   b. applying for a licence or informing the EPA of an allegation, complaint or issue
   c. paying for a service by credit card
   d. taking a test or responding to questions or surveys

   Note: Information provided to the EPA is usually done with the individual's knowledge and is the preferred way to collect personal information.
2. **Observed** information may be placed in the EPA records, as relevant to other information provided e.g. details from online cookies, or closed-circuit television footage in public places (if combined with facial recognition).
3. **Derived** data is mechanically collected e.g. the number of times a website is visited, how often a service is requested, or some other arithmetic process applied to data to predict future demand for services.
4. **Inferred** data collection may occur where statistical information is based on current personal information held by the EPA e.g. response scores, number of services requested, or in projects where "big data" is used to generate insights into future needs.

Note: Inferred information is likely to be so de-identified that it would be impossible to identify specific individuals.

The EPA takes reasonable steps to ensure the personal information it holds:

- is relevant to the purpose for which it has been collected
- is not excessive
- is accurate, up to date and complete
- does not unreasonably intrude into an individual's personal affairs.

Managing privacy during collection

When collecting personal information, the EPA will explain:

- that personal information is being captured, and the way it is being collected
- why the EPA is collecting the information
- the intended user(s) and/or recipients of the information
- that personal information will not be disclosed or transferred without consent, unless the EPA is lawfully authorised or required to do so
- if there is a legal requirement to provide the information to the EPA, and the consequences of not providing the information
- if there is no legal requirement, that the information is being provided voluntarily
- that individuals may have the right to access, modify and suppress their personal information.

The above details are usually included in a privacy statement on the application or questionnaire forms used to collect the personal information or on the EPA website when seeking submissions.

Developing forms and documents

The EPA is committed to ensuring the privacy and security of its website and online newsletters.

Employees must be responsible for designing forms in web-based transactions or other instruments to ensure they include adequate advice about the EPA privacy management procedures, contact details and seek advice from the EPA Risk and Governance team where appropriate.

5.2. Storing personal information (IPP 5)

All the EPA's business units apply appropriate security to protect personal information through all stages of its life cycle.

To help protect and keep personal information secure, the EPA:

- uses password protection on departmental devices and multi-factor authentication for additional security
- stores records in an approved electronic document records management system (EDRMS)
- does not keep personal information any longer than is necessary
- securely disposes of personal information if no longer required, and ensures it is protected from misuse.

The departmental Records and Information Management Policy, the *State Records Act 1998* and the relevant standards provide guidance on storing information. Records must be kept for minimum retention periods specified in Retention and Disposal Authorities issued by State Records NSW.

5.3. Accessing personal information held by the EPA (IPPs 6–7)

Individuals can find out if the EPA holds their personal information by contacting the Risk and Governance team. See *Appendix A1.3: Advice*.

The Risk and Governance team can advise whether the EPA holds their personal information, the nature of the personal information and the main purposes for which it is used.

Individuals can request access to their personal information. Access is usually provided within 20–30 working days of receiving a request, with minimal cost. If there is likely to be a delay, the EPA will explain this and advise when the information may be available.

Individuals can also apply directly to the relevant EPA business area holding their information if they know the business area.

5.4. Refusal of access and the Government Information (Public Access) Act 2009

The PPIP Act provides that public sector agencies that hold personal information must, at the request of the individual to whom the information relates, provide the individual with access to the information. There are some exemptions, set out in section 8 below.

If the EPA refuses access under the PPIP Act, it will provide the individuals with reasons.

Access to personal information can also be requested under the *Government Information (Public Access) Act 2009* (GIPA Act).

Section 5 of the PPIP Act states nothing in the Act affects the operation of the GIPA Act. This means the PPIP Act does not override the GIPA Act or lessen any obligations under the GIPA Act in respect of a public sector agency.

5.5. Amending personal information (IPP 8)

Individuals can request their personal information held by the EPA be amended if they believe it is:

- inaccurate or irrelevant
- out of date
- incomplete and/or misleading.

To amend their information, individuals need to provide evidence to demonstrate the information is inaccurate, irrelevant, not up to date, incomplete and/or misleading. See *Appendix A1.3: Advice* for where to send a request.

The EPA decides if it is appropriate to amend personal information within 20–30 working days of receiving a request.

Refusal to amend

If the EPA refuses to amend personal information, the reasons will be provided, and the EPA may attach a notation to the information, indicating the amendment sought.

If the request for amendment is denied, individuals have rights of internal review under the PPIP Act. See *10: Complaints and internal reviews*.

5.6. Using personal information (IPPs 9–10)

Before using personal information, the EPA will ensure it is accurate, up to date, relevant, complete and not misleading. If it has been a while since the information was collected, or there are other reasons to doubt the adequacy of the information, the EPA will take reasonable steps to verify the authenticity of the information.

Personal information is only used for the purposes for which it was collected. If it needs to be used for another purpose, consent will be obtained. One exception to this is where the information is used to prevent danger to someone or in other specific situations. See *8: Exemptions under the PPIP Act*.

5.7. Disclosing personal information (IPPs 11–12)

The EPA may only disclose personal information to other parties for a purpose other than the one for which it was collected, if the:

- owner of the personal information consents
- owner of the personal information is aware this type of information is usually disclosed in the way it's being disclosed
- secondary purpose is directly related to the purpose for which it was first collected, or
- information is supplied to prevent danger to someone.

This means EPA employees do not disclose personal information to a third party without consent, unless in other specific situations as set out in the PPIP Act apply. See *7: Modifications to the PPIP and HRIP Acts*.

In addition, the EPA does not disclose:

- information relating to a person's ethnic or racial origin, political opinions, religious or philosophical beliefs or trade union membership, except to prevent death or injury
- personal information to anyone outside NSW unless there are similar privacy laws in that individual's jurisdiction, or the disclosure is allowed under a privacy code of practice, or under legislation such as the HRIP Act and the PPIP Act.

The EPA may disclose information without consent, if:

- the disclosure will benefit the individual, and
- it is impracticable to obtain consent, and
- if the EPA could obtain consent, it is likely it would be given
- an exemption under the PPIP Act applies.

6. Application of the Health Privacy Principles (HPPs)

The HRIP Act states how the EPA must protect the health information it holds. The same Act also enables individuals to gain access to their health information. There are 15 Health Privacy Principles (HPPs) listed in the HRIP Act.

6.1. Collecting health information (HPPs 1–4)

The EPA only collects health information for a lawful purpose directly related to its work, which is reasonably necessary to carry out the EPA's functions or as part of dealing with unwell EPA staff. The information is collected directly from individuals unless it's unreasonable or impracticable to do so.

When the EPA collects health information, it applies the principles for the collection of personal information as outlined above for IPPs 1–4.

If the health information collected about an individual is provided by someone else, the EPA will ensure the person to whom the information relates is made aware of this fact and has consented.

The only time the EPA would not follow these principles is if:

- it would pose a serious threat to the life or health of any individual
- the collection is made in accordance with guidelines issued by the Privacy Commissioner, or
- the HRIP Act or other legislation provides an exemption.

6.2. Storing health information (HPP 5)

The EPA applies appropriate security to protect the health information it holds. The security of information extends to all stages of the information life cycle.

To help protect and keep personal information secure, the EPA:

- uses password protection on departmental devices and multi-factor authentication for additional security
- stores records in an approved electronic document records management system (EDRMS)
- does not keep personal information any longer than is necessary
- securely disposes of personal information if no longer required, and ensures it's protected from misuse.

The departmental Records and Information Management Policy, the *State Records Act 1998* and the relevant standards provide guidance on storing information. Records must be kept for minimum retention periods specified in Retention and Disposal Authorities issued by State Records NSW.

6.3. Accessing health information (HPPs 6–7)

Individuals can find out if the EPA holds their health information by contacting the Risk and Governance team. See *Appendix A1.3: Advice*.

The Risk and Governance team can advise whether the EPA holds their health information, the nature of the health information and the main purposes for which it is used.

Individuals can request access to their health information. Access is usually provided within 20–30 working days of receiving a request. If there is likely to be a delay, the EPA will explain this and advise when the

information may be available. A fee may be charged for providing a copy of health information. The fee payable will depend on the circumstances of each request.

Individuals can also apply directly to the relevant business area holding their information if they know who that is.

Refusal of access and the GIPA Act

If the EPA refuses a request to access health information, it will provide detailed reasons to the individual in writing.

Individuals can also request access to their personal information under the *Government Information (Public Access) Act 2009* (GIPA Act).

Section 22 of the HRIP Act states nothing in the Act affects the operation of the GIPA Act. This means the HRIP Act does not override the GIPA Act or lessen any obligations under the GIPA Act in respect of a public sector agency.

6.4. Amending health information (HPP 8)

Individuals can ask the EPA to amend any health information it holds about them if they believe it is:

- inaccurate or irrelevant
- out of date
- incomplete and/or misleading.

To amend their information, individuals need to provide evidence to demonstrate the information is inaccurate, irrelevant, not up to date, incomplete and/or misleading.

The EPA decides if it's appropriate to amend health information within 20–30 working days of receiving a request.

Refusal to amend

If the EPA refuses to amend health information, the reasons will be provided, and the EPA may attach a notation to the information, indicating the amendment sought.

If the request for amendment is denied, individuals have rights of internal review under the HRIP Act. See *10: Complaints and internal reviews*.

6.5. Using health information (HPPs 9–10)

Before use, the EPA will ensure health information is accurate, up to date, relevant, complete and not misleading. If it has been a while since the information was collected, or there are other reasons to doubt the adequacy of the information, the EPA will take reasonable steps to verify the authenticity of the information.

Health information is only used for the purposes for which it was collected. If there is a need to use the information for another purpose, consent will be obtained. One exception to this is where the information is used to prevent danger to someone or in other specific situations set out in the HRIP Act.

A list of the other exemptions is provided under section *9: Exemptions under the HRIP Act below*.

6.6. Disclosing health information (HPP 11)

The EPA can only disclose health information to other parties for a purpose other than the one for which it was collected, if the:

- owner of the health information consents
- secondary purpose is directly related to the purpose for which it was first collected, or
- information is supplied to prevent danger to someone
- secondary purpose is reasonably necessary for the funding, management, planning or evaluation of health services or for training, research or for other reasons set out in the HRIP Act, or
- exceptions set out in the HRIP Act are established.

See *9: Exemptions under the HRIP Act*.

6.7. Identifiers (HPP 12)

A healthcare identifier is a number that uniquely identifies either a healthcare provider or a healthcare recipient.

The EPA may assign identifiers to **individuals** if it is reasonably necessary to enable the EPA to carry out its functions efficiently.

In certain circumstances, identifiers can be adopted by a private sector person to carry out certain functions. Identifiers may also be disclosed and used if consent is given by the individual to whom the information relates.

6.8. Anonymity (HPP 13)

Individuals can be given the opportunity to remain anonymous when entering a transaction with the EPA if it is lawful and practicable to do so.

6.9. Providing data to persons or bodies outside NSW (HPP 14)

In certain circumstances, the EPA may provide health information to a:

- person or body outside NSW jurisdiction, or
- Commonwealth agency.

This will only occur where:

- it is a legal requirement and upholds the HPPs
- the individual to whom the information relates has consented to the transfer
- it is necessary to do something requested by the individual to whom the information relates
- it is reasonably necessary to lessen/prevent an imminent threat to the life, health or safety of a person
- the EPA has taken reasonable steps to ensure it will comply with the HPPs
- the transfer is permitted or required by legislation or law, or
- a situation where all the following apply:
  a. the transfer is for the benefit of the individual to whom the information relates
  b. it's impracticable to obtain consent, and
  c. if it were practicable to obtain consent, it would probably be given.

6.10. Linkage of health records (HPP 15)

Unless the individual has consented to the linkage, the EPA must not include an individual's health information or disclose an identifier about an individual in a health linkage system.

Sometimes it may be lawful for the EPA not to comply with HPP15. This is if non-compliance is permitted under another Act or law, or if the linkage complies with HPP 10(1)(f) and the disclosure complies with HPP 11(1)(f).

7. Modifications to the PPIP and HRIP Acts

7.1. Public registers

Under the PPIP Act, a public register is a register of personal information required by law to be, or is, made publicly available or open to public inspection.

Information on public registers is only made available for legitimate purposes, that is, a purpose relating to the reason for the register to exist, or of the Act or legislation under which the register is kept.

The EPA maintains several public registers and databases, as required by legislation. Public registers are found on the EPA website: https://epa.nsw.gov.au/publicregister/.

The EPA is covered by the *Privacy Code of Practice (General) 2003* (the Code) in respect of modification of Part 6 of the PPIP Act and the public registers kept by the EPA.

Schedule 2 of the Code limits the information required to be published on the public registers in respect of various Acts the EPA administers.

The EPA is the regulator under the *Plastic Reduction and Circular Economy Act 2021* (PRCE Act). As the regulator, the EPA is required to keep a public register of information as prescribed in the PRCE Act. The EPA will include appropriate statements on the website requiring those accessing the registers to use such information only for a purpose relating to the register or the PRCE Act.

Right to request personal details be suppressed

Any person with personal information recorded in a public register has the right to request their personal details be suppressed. If someone wants their personal information to be suppressed, they can contact the Risk and Governance team to apply. See *Appendix A1.3: Advice*.

7.2. Directions of the Privacy Commissioner

Under section 41 of the PPIP Act and section 62 of the HRIP Act, the Privacy Commissioner may make a direction to waive or modify the requirement for a public sector agency to comply with:

- an information protection principle
- a health privacy principle
- a privacy code of practice.

Agencies can approach the Privacy Commissioner to request a Direction. The general intent is for Directions to apply temporarily. If a longer-term waiver or modification in the application of an IPP or HPP is sought, then a code of practice may be more appropriate.

Some previous Directions have been incorporated in legislation, including the PPIP Act. Directions currently in operation are listed on the website of the Privacy Commissioner.

7.3. Privacy Code of Practice

Under the PPIP Act, codes of practice may be created to allow an agency to modify the application of one or more Information Protection Principles or specify how they are to be applied to activities or classes of information. The Privacy Code of Practice (General) 2003 applies to the EPA in respect of environmental offences involving vehicles (Schedule 1).

This means the EPA may contact the owner (operator) of a vehicle when it has received a report about an environmental offence concerning the vehicle. Transport for NSW may exchange the details of the vehicle's registered owner with the EPA for this purpose.

8. Exemptions under the PPIP Act

Both the PPIP Act and the HRIP Act provide some specific exemptions from the IPPs and the HPPs.

Table 1 below shows the exemptions listed under sections 23–28 of the PPIP Act. Some of these are further detailed below.

Table 1 PPIP Act exemptions from the IPPs

Subject	Section
Law enforcement and related matters	23
ASIO related	23A
Investigative agencies	24
Lawfully authorised or required	25
Benefiting the individual	26
Exemptions relating to ICAC, NSW Police, Police Integrity Commission and the NSW Crime Commission	27
Exchanges between public sector agencies	27A
Research	27B
Credit information	27C
Emergency situations	27D
Other exemptions	28

8.1. Law enforcement purposes

Section 23(6A) of the PPIP Act provides an exemption to a public sector agency if the collection, use or disclosure of the information to another public sector agency is reasonably necessary for law enforcement purposes. Law enforcement purposes are not defined in the PPIP Act.

Law enforcement purposes may include (section 6 *Privacy Act 1988* (Clth)):

- prevention, detection, investigation, prosecution or punishment of offences or breaches of a law imposing a penalty or sanction
- conduct of surveillance, intelligence gathering or monitoring activities
- preparation for, or conduct of, proceedings before a court or tribunal, or implementation of orders of a court or tribunal.

8.2. Investigative agencies

Section 3 of the PPIP Act defines the term ‘investigative agencies’. This covers NSW public sector agencies with investigation functions if their functions are:

- exercisable under the authority of an Act or statutory rule, and
- may result in the agency taking or instituting disciplinary, criminal or other formal action or proceedings against a person or body under investigation.

Section 24 of the PPIP Act specifies the scope of the exemptions relating to investigative agencies.

8.3. Lawfully authorised

Section 25 of the PPIP Act provides an exemption if the collection, use or disclosure of the information by a government sector agency is ”lawfully authorised”. This term has been considered in various tribunal matters, including issues around:

- disclosure within the terms of a subpoena
- the requirement to notify a person against whom a complaint has been made
- informing a trade union official in respect of various issues under legislation
- disclosures to the Anti-discrimination Board, or other such boards or commissions

Some requirements under legislation appear to allow for the disclosure of personal information; however, staff must take great care, and assess whether non-compliance with the IPPs is lawfully authorised.

8.4. Benefiting the individual

Section 26 of the PPIP Act provides an exemption where non-disclosure would prejudice the interests of the individual to whom the information relates or there has been express consent for another use or disclosure.

Consent is only genuine if individuals have the capacity to give or withhold consent. For consent to be valid it must be voluntary, informed, specific and current. Notifying individuals of the EPA’s intention to deal with their personal information is not consent.

The section also provides that a public sector agency is not required to comply with some IPPs if the individual to whom the personal information relates has expressly consented to the agency not complying with the principle concerned.

8.5. Exemptions relating to ICAC, NSW Police, Police Integrity Commission and the NSW Crime Commission

Section 27 of the PPIP Act provides that these agencies are not required to comply with the IPPs, except in connection with their administrative and educative functions.

8.6. Exchanges of information between agencies

Section 27A of the PPIP Act provides an exemption relating to information exchanges between public sector agencies. Information can be provided to or by another public sector agency if it is reasonably necessary to:

- allow any of the agencies concerned to deal with, or respond to, correspondence from a Minister or Member of Parliament
- enable inquiries to be referred between the agencies concerned, or
- enable the auditing of the accounts or performance of the agency.

This may occur where one agency has applied to an agency for a service, and another agency needs to provide a response.

Employees should seek consent from the person involved, if possible, and/or ask for advice from the EPA Governance team. See *Appendix A1.3: Advice*.

Memorandum of Understanding (MOU) or referral arrangements

The EPA does not have any formal referral arrangements in place with agencies in NSW. However, the following MOUs exist for the exchange of information with other agencies that may affect the operation of the PPIP and HRIP Acts:

- An MOU between the EPA and Roads and Maritime Services (RMS) allows the EPA to have access to DRIVES, which is RMS' database of driver licensing and vehicle registration data. It includes personal information regulated under the PPIP Act and the Road Transport Law Confidentiality provisions.
- An MOU between NSW Police Force (NSWPF), EPA and Department of Planning, Housing and Infrastructure (DPHI) allows for the exchange of information between all Parties for enforcement or investigation purposes as well as proactively notifying and providing information of a conviction or a guilty conviction of NSWPF or EPA or DPHI.
- An MOU between the EPA and Transport for NSW (TfNSW) for investigation of offences concerning smoking vehicles, noisy vehicles and littering from vehicles allows TfNSW to release to the EPA the name and address of the registered operator of the vehicle under investigation. TfNSW is permitted to release such information under the law enforcement exception in section 23(5) of the PPIP Act.

8.7. Research

Section 27B of the PPIP Act provides an exemption relating to research. Statutory guidelines on research have been published by the Information and Privacy Commission:

https://www.ipc.nsw.gov.au/media/556

8.8. Other exemptions

Section 28 of the PPIP Act describes other exemptions relating to various agencies, including an exemption for any public sector agency if the disclosure is to inform the Minister or the Premier about any matter within their administration.

These exemptions should only be relied on after seeking advice. See *Appendix A1.3: Advice*.

9. Exemptions under the HRIP Act

Each of the HPPs in the HRIP Act list circumstances when the EPA is not required to comply with the principles. These include:

- where lawfully authorised or required (cl 10(2)(a) of Sch 1)
- where non-compliance is otherwise permitted under an Act or any other law (cl 10(2)(b) of Sch 1)
- there is a serious threat to health or welfare (cl 10(1)(c) of Sch 1)
- the use for a secondary purpose, such as management of health services, training and/or research only where it's not possible to carry out that purpose using de-identified information and it's not reasonably practicable to seek consent (cl 10(1)(d), (e) and (f) of Sch 1)
- finding a missing person (cl 10(1)(g) of Sch 1)
- suspected unlawful activity or conduct grounds for disciplinary action (cl 10(1)(h) of Sch 1).

Individuals may consent to the EPA not complying with any or some of the IPPs or the HPPs in certain circumstances. See *8.4 Benefiting the individual*.

10. Privacy complaints, breaches and internal reviews

If individuals believe the EPA may have breached an information protection principle or health privacy principle, or has not complied with a request for access or amendment, they can:

- raise a complaint with the EPA
- apply for an internal review
- lodge a complaint with the Information and Privacy Commission.

If there is a mechanism for internal review within a public sector agency, the Privacy Commissioner may only make recommendations and not investigate complaints regarding alleged conduct of that agency.

10.1. Raising a complaint (informal)

If individuals want to raise an issue informally, they can contact the relevant area, if known. Complaints may be handled under relevant guidelines for handling external complaints, if appropriate: see the EPA's Complaint Handling Policy.[1] Informal complaints are dealt with by EPA officers and there are no formal review rights. Check costs in advance: if there are fees, they may be waived or reduced in certain circumstances.

10.2. Raising a complaint (formal)

If individuals want to take a more formal approach, they can refer the complaint for an internal review. Under the HRIP Act and the PPIP Act, complaints or applications for internal review:

- should be lodged within six months of becoming aware of the legal implications/significance of the alleged conduct
- should be in writing
- must have a return address in Australia.

An EPA officer who is not substantially involved in the subject matter of the complaint conducts the review. They are responsible for reviewing the action or decision and deciding if it was correct. Reviews must be conducted within 60 days.

If the EPA doesn't complete the internal review within the 60 days, an appeal may be lodged with the Administrative and Equal Opportunity Division of the NSW Civil and Administrative Tribunal (NCAT) within 28 days after the report was due.

Also, individuals may appeal against the result of an internal review with the NCAT.

Appeals may be lodged with the NCAT within 28 days after receiving the report. The NCAT can be contacted on 1300 006 228.

The EPA internal review process is set out in Procedure 2. The EPA Complaint Handling Policy is not applicable to formal privacy complaints, as the PPIP Act prescribes the applicable process.

The Privacy Commissioner may make recommendations in respect of the EPA internal review process.

There is no cost to lodge a complaint or to request an internal review.

[1] https://www.epa.nsw.gov.au/publications/whoweare/epa-complaint-handling-policy

Procedures

P1 Breach of privacy or data breach notification

Affected individuals will be notified in the event of a serious data breach.

A serious data breach means unauthorised access to, unauthorised disclosure of, or loss of, personal information held by the EPA, resulting in a real risk of serious harm to any of the individuals to whom the information relates.

A less serious breach may occur when there is a failure that has caused, or has the potential to cause, unauthorised access to data, such as:

- accidental loss or theft of classified data, or equipment on which such data is stored
- unauthorised use, access to or modification of data or information systems
- compromised user account e.g. through phishing
- unauthorised disclosure of classified data e.g. email sent to incorrect recipient, or posted to incorrect address or addressee, or published on website
- failed or successful attempts to gain unauthorised access to information
- equipment failure
- malware infection
- disruption to or denial of IT services.

Data breaches may result in unauthorised collection, use, disclosure or access to personal information. If this happens, the EPA will act quickly to contain the breach, evaluate the risks, consider notifying affected individuals and prevent a repeat.

Notifying individuals helps mitigate any damage to those people and reflects positively on the EPA. If the breach causes a risk of serious harm to them, they must be notified as soon as possible. The Privacy Commissioner should also be notified if the breach is serious.

A Breach of Privacy Notification template is set out below. It can be used to notify affected individuals, as well as the Privacy Commissioner, in cases of a serious privacy breach. Employees are to modify it to suit the relevant situation and should seek advice from the privacy experts within the agency.

* SAMPLE ONLY *

Use agency letterhead or customise an email to clearly show agency details

Dear [**name**]

I am writing to you with important information about a recent data breach involving your [*personal information* **or** *information about your organisation*].

We became aware of this breach on [*date*]. The breach occurred on or about [*date*] and occurred as follows:

[*Describe the event, including the following, as applicable:*

- *a brief description of what happened*
- *description of the data that was inappropriately accessed, collected, used or disclosed*
- *steps the individual/organisation should take to protect themselves from potential harm from the breach*

- *a brief description of what [agency name] is doing to investigate the breach, control or mitigate harm to individuals/organisations and to protect against further breaches.*]

Please call me with any questions or concerns you may have about the data breach.

[OPTIONAL – *We have established a section on our website [**insert link**] with updated information and links to resources that offer information about this data breach*.]

We take our role in safeguarding your data, and using it in an appropriate manner, very seriously. Please be assured we are doing everything we can to rectify the situation.

Please note you are entitled to register a complaint with the NSW Privacy Commissioner about this breach.

If you have any questions regarding this notice or if you would like more information, please contact me by telephone on [*number*], or via email [*email address*].

Yours sincerely,

[*Name, date and signature block*]

Mandatory notification of data breaches

Roles	Responsibilities
Executive Director, Legal, Governance and People Director, Governance, Risk and Planning	• Carry out or direct one or more persons to carry out an assessment of the data breach • Decide the nature of the data breach and the risks associated with the breach to determine next steps • Provide instruction to mitigate the harm done by the suspected breach • Approve extension of the period to conduct an assessment • Any other functions that are authorised by the EPA Chief Executive Officer (CEO) in accordance with the CEO delegation instrument.
Senior Leadership Team	• Make all reasonable efforts to contain the data breach • Ensure staff comply with training requirements on handling personal and health information • Assist with incident review and preventative efforts, based on the type and seriousness of the breach.
Risk and Governance team members	• Liaise with the NSW Information and Privacy Commission and affected individuals • Maintain an internal register for eligible data breaches • Maintain a public register of data breach notifications issued • Review and update the EPA Mandatory Reporting of Data Breaches Policy • Review and update other policy and procedure documents including this Privacy Management Plan.
All EPA employees	• Handle personal information in accordance with the *Privacy and Personal Information Protection Act* • Label sensitive information in accordance with *NSW Government Information Classification, Labelling and Handling Guidelines* • Undertake required training on handling personal and health information • Take steps to ensure external stakeholders comply with our privacy requirements • Report all data breaches and suspected data breaches • Assist with investigating and assessing breaches, and any resulting internal reviews.

P2 Internal review procedures

Any complaint or request for an internal review regarding a privacy matter is to be sent to the relevant privacy officer. A senior reviewing officer will assess the application.

The reviewing officer is also responsible for deciding if late applications will be accepted or not. If it is not accepted, the applicant must be advised of the reasons and how their complaint will be handled instead, as well as their right to complain to the Privacy Commissioner.

Notifying the Privacy Commissioner

When an application for an internal review is made, the EPA is required to notify the Privacy Commissioner as soon as practical after receiving the application.

Assessing the application

When assessing the application, the reviewing officer will check to confirm:

- it is about personal information in relation to conduct occurring after 1 July 2000, or
- it is about health information in relation to conduct occurring after 1 September 2004, and
- it has been lodged within 6 months of the applicant becoming aware of the legal implications or significance of the alleged conduct.

If the application doesn't meet these criteria, it may be referred to relevant managers for handling under the EPA complaint handling procedures.

Review procedure

If the criteria are met, the reviewing officer:

1. writes to the applicant within 14 days of receiving the application stating:
    - the officer's understanding of the complaint
    - the officers understanding of the privacy principle(s) at issue
    - an internal review is being conducted under the PPIP Act and/or the HRIP Act, as appropriate
    - the reviewing officer's name, title and contact details
    - that the reviewing officer is independent of the person(s) causing the complaint (more detail can be provided in the review report)
    - the estimated completion date for the review process
    - that if the review is not completed within 60 days of the date the review application was received, the applicant can go to the Administrative and Equal Opportunity Division of the NSW Civil and Administrative Tribunal (NCAT) for an external review of the matter
    - that a copy of the letter will be provided to the Privacy Commissioner, who has an oversight role
2. sends a copy of the above letter to the Privacy Commissioner
3. reviews the situation to determine whether the alleged conduct occurred, and if so, whether it constituted an unauthorised breach of the relevant privacy legislation.

    Note: If the review isn't finalised within four weeks of the issuing of the letters at steps 2 and 3, the reviewing officer will send a progress report to the applicant, copied to the Privacy Commissioner, that includes:
    - details progress to date
    - advises of any anticipated delays, the reasons for these, and a revised estimated completion date for the review process
    - a reminder that if the review is not completed by this new date (which, by then, is likely to be later than 60 days from the date the application for review was received), the applicant can go to NCAT for an external review of the alleged conduct

4. on completion of the review, writes a draft report:
    - detailing review findings about the facts, the law and the reviewer's interpretation of the law
    - giving a determination as to if a breach has occurred, with one of the following findings:
        - there was insufficient evidence to suggest alleged conduct occurred
        - alleged conduct occurred but complied with the privacy/health privacy principles and/or public register provisions
        - alleged conduct occurred, but the non-compliance was authorised by an exemption, Code or Direction (section 41 of PPIP Act or section 62 of HRIP Act)
        - alleged conduct occurred and did not comply with principles or public register provisions and was not authorised, and so constitutes a "breach" of the legislation
5. makes recommendations on appropriate action by way of response or remedy e.g. an apology, changing agency processes, providing training to relevant employees, etc.
6. sends a copy of the draft report to the Privacy Commissioner for comment, and see if they want to make a submission
7. finalises the report, taking into consideration any comments or recommendations provided by the Privacy Commissioner, and submit for endorsement by the relevant Senior Executive
8. notifies the complainant and the Privacy Commissioner in writing:
    - that the review is finished
    - of the review findings (and the reasons and legislative basis for those findings), and any action proposed to be taken
    - of the right to apply within 28 days to the Administrative and Equal Opportunity Division of the NSW Civil and Administrative Tribunal (NCAT) for a further review, providing contact details for the NCAT.

P3 Privacy notices and consent

If the EPA:

- **does** intend to use/disclose personal information, consent from the individual may be required
- **does not** intend to use/disclose the personal or health information, no consent is required.

The Fact Sheet – Consent provides useful information on when and how to seek consent.

Verbal collection of information

Verbal collection of information (e.g. during telephone discussions) means the EPA can use less formal wording. When collecting information verbally, it's important to explain:

- **how** the person's personal information will be used, and
- **to whom** the EPA is likely to disclose it.

It is also important to make a file note of what was said and record it in an EDRMS for the full and accurate capture of records as per the State Records Act12 (1)..

If the person asks if the information is really needed, the EPA can go into more depth, mention the person's access and amendment rights and/or offer to let them speak with the Risk and Governance team. See *Appendix A1.3: Advice*.

Consent to a secondary use or disclosure of information

If a person's verbal consent to a secondary use or disclosure is required, the EPA must:

- provide an explanation of what the EPA is asking
- ensure the person understands they are free to say 'no'

- make a file note of what was said and record it in an EDRMS for the full and accurate capture of records as per the State Records Act 12 (1).

Written collection of information

When collecting personal information, the EPA needs to inform the person of the following:

- the EPA contact details
- who will hold and/or have access to the information
- what it will be used for (the purpose of collection)
- what other organisation, if any, routinely (or may) receive this information from the EPA (this should include the possibility of the Data Analytics Centre receiving de-identified data)
- whether the collection is voluntary or required by law
- if the EPA is likely to disclose the information to anyone overseas and, if so, the countries the information may be going to (e.g. cloud-based information services, overseas provider of services)
- how the person can access and request amendment of their personal information held by the EPA
- if the EPA has obtained the information from someone else, or it's unlikely the person realises the EPA has collected information, what the EPA collects, or has collected, and the circumstances of collection.

When personal information is collected and will be used or disclosed by the EPA, use the template notice below. It can be amended to suit the purpose and advice can be sought internally from the appropriate privacy expert. See *Appendix A1.3: Advice*.

Template notice for written consent

SAMPLE ONLY

[*Name of agency*] is requesting this information from you so the EPA can [*describe the purpose of collection – e.g. providing a service, lodging an application etc*.].

The EPA may also [*describe any directly related purpose for which the information might be used – e.g. reporting or program evaluation, publishing summary of submissions*].

For the same purpose, [*Agency name*] may provide this information about you to [*list any persons or organisations that such information is usually disclosed to, outside of the agency – e.g. a contractor or consultant, a service provider etc*.].

[OPTIONAL PARAGRAPH] When storing your personal information electronically, [*agency name*] may disclose your personal information to overseas recipients by virtue of its cloud computing arrangements.

The EPA 'cloud' servers are in [*names of countries*] and [*name of agency*] is reasonably satisfied these countries have similar privacy protections to those afforded under Australian law.

The EPA will not disclose your personal information to anybody else, unless you have given consent, or the EPA is required to do so by law. The *EPA Privacy Management Plan* describes when this might occur, particularly sections 7.6 and 9.

Providing the EPA with the requested information is not required by law. If you choose not to provide it … [*describe the main consequence – e.g. unable to process application or investigate complaint*].

You may request access to your information at any time. To access or update your information, or for more details on EPA privacy obligations, please contact [*Name, email and website where privacy management plan can be found*].

Secondary purpose consent

When seeking consent to be able to use information for a secondary purpose, the following statement could be used:

SAMPLE ONLY

With your permission, the EPA would also like to [*use/disclose*] your information to [*describe intended secondary purpose – e.g. put on mailing list*].

I consent to my personal information being [*used/disclosed*] for the purpose of [*name of secondary purpose*].

Signature [*of person giving consent*]: _____Date: _____

Name [*of person giving consent*]: _____

Appendix A: Definitions and resources

A1.1 Defined terms

In this plan:

'Bundled consent' refers to the practice of putting together multiple requests for consent to a wide range of collections, uses and disclosure of personal information, without giving individuals the opportunity to choose which collections, uses and disclosures to which they do or do not agree.

It undermines the voluntary nature of the consent and should not be used in a privacy statement or consent request.

'Express consent' means a person gives consent openly and obviously, either verbally or in writing.

'**Health information'** means information or an opinion about:

- a person's physical or mental health or a disability (at any time)
- a person's express wishes about future provision of health services to him or her
- a health service provided, or to be provided, to someone
- other personal information collected relating to provision of a health service
- a person's organ, body parts or body substances donation i.e. genetic information held arising from health service provisions that may predict their health or the health of one of their relatives.

'Implied consent' arises where it may be reasonably inferred in the circumstances from the person's conduct. Silence is not consent. If individuals do not object to giving consent, it doesn't mean they have given consent.

'Personal information' has the same meaning as provided in section 4 of the PPIP Act. However, for the purposes of this plan, 'personal information' includes 'health information' in all applicable instances, unless otherwise specified.

A1.2 Legislation, obligations and related documents

The key legislation relevant to privacy includes:

- *Anti-Discrimination Act 1977*
- *Crimes Act 1900*
- *Government Information (Public Access) Act 2009*
- *Government Sector Employment Act 2013*
- *Health Records and Information Privacy Act 2002*
- *Privacy and Personal Information Protection Act 1998*
- *Public Interest Disclosures Act 1994*
- *State Records Act 1998*
- *Workplace Surveillance Act 2005.*

Other legislation that may affect personal and/or health information/records includes:

- *Contaminated Land Management Act 1997*
- *Dangerous Goods (Road and Rail Transport) Act 2008*
- *Environmentally Hazardous Chemicals Act 1985*
- *Environmental Planning and Assessment Act 1979*
- *Forestry Act 2012*
- *National Environment Protection Council (New South Wales) Act 1995*
- *Ozone Protection Act 1989*
- *Pesticides Act 1999*
- *Plastic Reduction and Circular Economy Act 2021*
- *Protection of the Environment Administration Act 1991*
- *Protection of the Environment Operations Act 1997*
- *Radiation Control Act 1990*
- *Recreation Vehicles Act 1983*
- *Waste Avoidance and Resource Recovery Act 2001.*

Related policies, as issued from time to time are:

- *EPA Information Guide 2022*
- *EPA Code of Ethics and Conduct*
- *DPE Acceptable Use Policy*
- *Records and Information Management Policy*
- *EPA Public Interest Disclosures Policy and Procedures 2022.*

A1.3 Advice

1. Contact the EPA Risk and Governance team if you want:
   - information about this privacy plan
   - to request information under the PPIP Act, HRIP Act or the GIPA Act
   - to ask for amendment of personal or health information.

   Environment Protection Authority (EPA)

   By telephone: (02) 9995 6497 or 9995 6099

   Via email: gipa.privacy@epa.nsw.gov.au

   By mail: Locked Bag 5022 Parramatta NSW 2124

   In person: 6 Parramatta Square, 10 Darcy Street Parramatta NSW 2150

   Website: https://www.epa.nsw.gov.au

2. Contact the Office of the Privacy Commissioner if you wish to make a complaint about an alleged breach of privacy or if you want advice on the:
   - PPIP Act
   - HRIP Act.

Contact the Office of the Information Commissioner if you want advice on the:

- GIPA Act.

NSW Information and Privacy Commission

Phone: 1800 472 679

Email: ipcinfo@ipc.nsw.gov.au

Postal Address – GPO Box 7011, Sydney NSW 2001

Street Address – Level 15, McKell Building, 2-24 Rawson Place, Haymarket NSW 2000

Website: www.ipc.nsw.gov.au

3. Individuals can lodge an appeal with the NCAT. A privacy matter would be dealt with by the Administrative and Equal Opportunity Division of the NCAT.

NSW Civil and Administrative Tribunal (NCAT)

Phone: 1300 006 228

Postal address – PO Box K1026, Haymarket NSW 1240

Street Address – Level 10, John Maddison Tower, 86–90 Goulburn Street, Sydney

Website: http://www.ncat.nsw.gov.au/

A1.4 Review

Governance, Risk and Planning will review this plan at least every three years, or more frequently on a needs-basis e.g. a change in legislation.

Appendix B: Responsibilities, reporting and record keeping

B2.1 Responsibilities

The table below describes roles and responsibilities expected from EPA employees, the Risk and Governance team and the Senior Leadership Team to help ensure this plan is implemented.

All EPA employees should comply with the Privacy Management Plan and associated procedures.

Table 2 Roles and responsibilities

Role	Responsibility
Senior Leadership Team	• Establish and maintain policies, systems and procedures for privacy management • Ensure mechanisms for responding to critical issues or risks arising are appropriate and effective • Ensure high-risk areas of work are identified and preventative strategies are in place • Make the Privacy Management Plan publicly available • Make employees aware of this plan and help them use it • Ensure employees are provided with access to privacy training and other development possibilities • Identify privacy issues when implementing new systems • Provide feedback regarding the effectiveness of the plan and suitable refinements to the Governance, Risk and Planning Branch as necessary.
Risk and Governance team members	• Reinforce compliance with privacy legislation • Report on privacy issues in the annual report • Advise and assist employees and the public in responding to requests for information • Support the plan through awareness-building, skills development and training • Help employees by providing advice and assistance regarding the plan, if required • Monitor the effectiveness of the plan and propose suitable refinements where appropriate