Office of the Victorian Information Commissioner

D19/8785

ovic.vic.gov.au | enquiries@ovic.vic.gov.au | 1300 006 842

Privacy Management Framework

Introduction

There are 10 Information Privacy Principles (**IPPs**) in the *Privacy and Data Protection Act 2014* (**PDP Act**) that set out the minimum standards and practices for handling personal information in the Victorian public sector.

Section 20 of the PDP Act states that an organisation must not do an act, or engage in a practice, that contravenes an IPP. It is the responsibility of all Victorian public sector organisations to implement appropriate measures to meet the requirements of the IPPs.

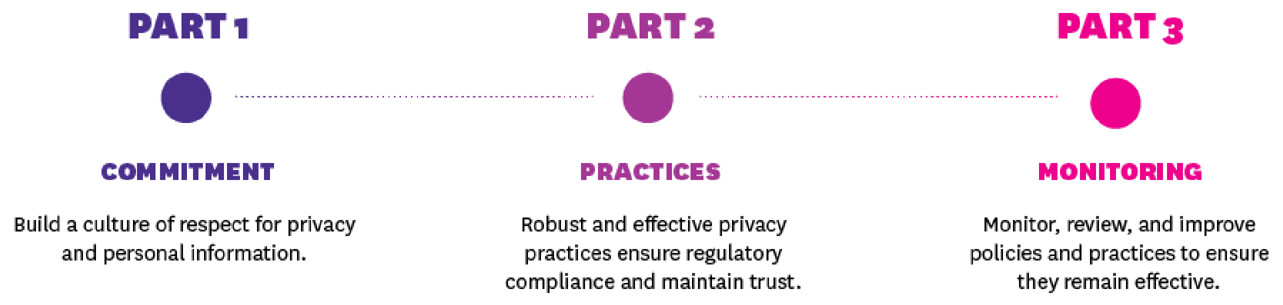
The measures an organisation implements will depend on a variety of factors, including the size of the organisation, its functions, the types of information it collects, and its relationship with the public.

Purpose

This Privacy Management Framework (**Framework**) is intended to provide organisations with guidance on the policies and procedures that promote good privacy practices within an organisation. The Framework encourages holistic information and privacy management by interconnecting a wide range of policies and information management tools.

Implementing the measures outlined in this Framework will enable an organisation to be accountable for its information handling practices, and convey to the public that it values and respects the privacy rights of individuals. The Framework will assist an organisation to demonstrate the steps it has taken to comply with the IPPs and section 20 of the PDP Act, and entrench a culture of privacy across the organisation.

This Framework is divided into three parts:



PART 1

COMMITMENT

Build a culture of respect for privacy and personal information.

PART 2

PRACTICES

Robust and effective privacy practices ensure regulatory compliance and maintain trust.

PART 3

MONITORING

Monitor, review, and improve policies and practices to ensure they remain effective.

The Framework includes links to resources, guides and templates containing further information to assist organisations in establishing and maintaining good privacy practices.

The end of this Framework also includes an organisational self-assessment checklist that can assist organisations to develop and maintain effective privacy management practices.

Note that organisations handling health information must also comply with the Health Privacy Principles contained in the *Health Records Act 2001* (Vic). This Framework does not discuss or consider those obligations.

Part 1 – Organisational commitment

Building a culture of respect for privacy and personal information across an organisation starts with good privacy governance and leadership.

1.1 An organisation ensures that its executive and senior management promote good privacy practices across the organisation. Using existing governance arrangements, such as boards, executive committees and management meetings to raise privacy issues and create general privacy awareness can be effective in creating an organisational culture that respects privacy.

1.2 An organisation should know and understand its privacy obligations. The Office of the Victorian Information Commissioner's (**OVIC**) *Guidelines to the Information Privacy Principles* detail how to interpret the IPPs in the PDP Act.

OVIC's Guidelines to the Information Privacy Principles

1.3 An organisation should consider if it has concurrent privacy obligations under the *Health Records Act 2001* (Vic), the *Charter of Human Rights and Responsibilities Act 2006* (Vic), the *Privacy Act 1988* (Cth), and other international laws.

Guidance from the Health Complaints Commissioner on the Health Records Act 2001

Australian Privacy Principle Guidelines under the Commonwealth Privacy Act 1988

Guidance on the Charter of Human Rights and Responsibilities Act 2006

Guidance for the Victorian public sector on the EU General Data Protection Regulation

1.4 An organisation should appoint key roles and responsibilities for privacy management, including a senior member of staff with overall organisational accountability for privacy. It should have staff responsible for managing day-to-day privacy, including a privacy officer or team, responsible for handling internal and external privacy enquiries, complaints, and providing advice to other staff on building privacy into their programs.

1.5 An organisation should ensure appropriate resourcing is allocated to maintain organisational privacy expertise relative to the organisation's nature, size, and complexity.

1.6 An organisation should ensure privacy is considered before, at the start of, and throughout the development and implementation of initiatives involving the collection, handling or use of personal information. It is important for an organisation to engage with its legal, procurement, and project teams to build privacy into contract and project documentation.

Implementing Privacy by Design

1.7 An organisation should understand the role of OVIC and its approach to using regulatory powers. OVIC's Regulatory Action Policy describes how it aims to promote, assure and enforce the PDP Act.

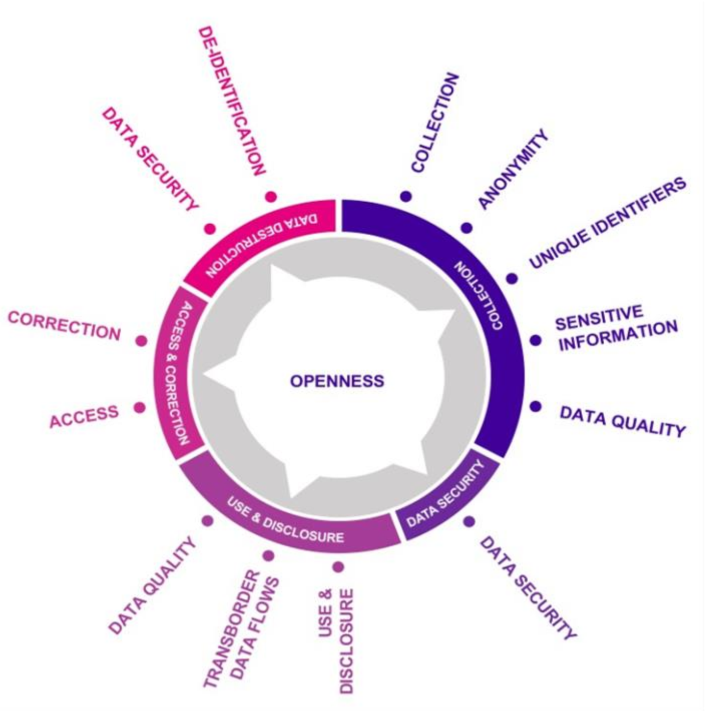
OVIC's Regulatory Action Policy

Part 2 – Privacy practices

Robust and effective privacy practices ensure regulatory compliance and maintain public trust in an organisation's ability to handle personal information.

2.1 An organisation should develop and maintain processes around handling personal information that align with the organisation's privacy obligations. Processes, procedures and policies need to be tailored to individual functions and activities an organisation undertakes.

2.2 An organisation's processes should cover the information lifecycle and clearly outline staff responsibilities when handling personal information. The information lifecycle is the flow of information from the point the organisation collects the information to the point the information is destroyed. The IPPs can be grouped into the five main stages of the information cycle. This is illustrated in the diagram.



2.3 An organisation should have a privacy policy that is current, easily accessible, easy to understand, and accurately reflects the organisation's practices.

IPP 5 – Openness: Organisation self-assessment tool

Understanding how to draft a privacy policy

2.4 An organisation should ensure reasonable steps are taken to give notice of the matters required under IPP 1.3 when collecting personal information. It is important to ensure steps taken to give notice (for example, a collection notice) are tailored to the circumstances, reviewed periodically, and consistent with the organisation's privacy policy.

Understanding how to draft collection notices

2.5 An organisation should ensure it is aware of any information security obligations it has under the Victorian Protective Data Security Framework. Privacy and security go hand-in-hand. Good information security practices protect personal information from unauthorised access, use, modification, or disclosure.

Guidelines to IPP 4.1 – Security of personal information

Victorian Protective Data Security Framework

2.6 An organisation should ensure Privacy Impact Assessments (**PIAs**) are undertaken for all projects and initiatives that involve personal information or impact on the organisation's information management practices or processes. PIAs should be reviewed and updated when material changes occur.

Privacy Impact Assessment guide and template

Getting executive buy-in for PIAs

2.7 An organisation should ensure it understands how and when personal information can be shared within and outside of the organisation, and how information should be protected when shared.

Guidelines for sharing personal information

Model terms for transborder data flows

Guidelines to IPP 2 – Using and disclosing personal information

2.8 An organisation should ensure the information handling practices of its contracted service providers (**CSPs**) adhere to the IPPs (or equivalent privacy protections) and align with the organisation's privacy obligations. Active steps should be taken to ensure CSPs have appropriate privacy practices in place.

Guidelines for outsourcing in the Victorian public sector

2.9 An organisation should implement a risk management process that enables the organisation to identify, assess and manage privacy risks across the organisation. Risks should be added to the organisation's risk register, and an accountable person assigned to manage risks.

2.10 An organisation should maintain a register (for example, in an organisational Information Asset Register) of the types of personal information it holds, where that information is located, and when it should be destroyed.

Guidelines on IPP 3 – Data Quality

Practitioner Guide: Identifying and Managing Information Assets

2.11 An organisation should have processes in place to ensure it monitors how long personal information should be retained before it is destroyed. Personal information must be destroyed or permanently de-identified when it is no longer needed for any purpose. Organisations should refer to the relevant Retention and Disposal Authority issued under the *Public Records Act 1973* (Vic) when determining whether data should be destroyed or permanently de-identified.

Guidelines to IPP 4.2 – Disposal of data

2.12 An organisation should incorporate privacy into staff inductions and conduct regular privacy training and awareness programs across the organisation.

OVIC face-to-face training – Information privacy under the Privacy and Data Protection Act 2014

OVIC online privacy module – Introduction to privacy in the Victorian public sector

OVIC online privacy module – Managing the privacy impacts of data breaches

2.13 An organisation should have a process for handling privacy enquiries and complaints. It should ensure stakeholders and the public know who to contact within the organisation or where to get help.

Responding to privacy complaints

2.14 An organisation should develop a data breach response plan and an incident management process. It should ensure staff know what to do and who to contact when a breach occurs. An organisation should be aware of the Information Security Incident Notification Scheme, which requires certain organisations to notify OVIC of incidents that compromise public sector information.

OVIC Information Security Incident Notification Scheme

Notifiable Data Breaches scheme under the Commonwealth Privacy Act 1988

Managing the privacy impacts of a data breach

2.15 An organisation should develop and implement a program of engagement and awareness activities to build and enhance a privacy conscious culture. This could include participating in Privacy Awareness Week activities, or conducting regular seminars or other events with privacy officers and experts that highlight good privacy practices.

Part 3 – Monitor, review, and improve

Monitor, review, and improve policies and practices to ensure they remain relevant and effective. Privacy is fast-moving and ever evolving which means organisations need to be proactive and anticipate future challenges.

3.1 An organisation should monitor and review its privacy policies and processes regularly to ensure they are up to date and fit for purpose. This should involve assessing its privacy policy, collection notices, and PIA templates – at least annually – to ensure they are up to date.

3.2 An organisation should establish a process to measure or evaluate the effectiveness of the organisation's privacy practices, processes, and resources. This could include measuring the awareness of good privacy practices and the adoption and use of privacy tools or resources across the organisation.

3.3 An organisation should regularly review its risk registers to ensure privacy risks are being appropriately managed.

3.4 An organisation should proactively examine the privacy implications, risks and benefits of new technologies it introduces into the organisation, and address identified risks. Where a new process or technology changes the organisation's information handling practices, any privacy policies, collection notices and PIAs should be updated to reflect those changes.

3.5 An organisation should ensure that any material changes to its privacy policies, procedures and practices are communicated appropriately to its employees and any relevant key stakeholders.

3.6 An organisation should document compliance with its privacy obligations including keeping records of privacy process reviews, breaches and complaints. These records should enable an organisation to identify systemic privacy risks, common themes, and opportunities for improvement. Any themes and privacy risks identified should be reported to senior management and those responsible for privacy.

3.7 An organisation should create a culture of continuous improvement by encouraging input from staff, the public, and key stakeholders with suggestions and feedback on the organisation's privacy practices.

3.8 An organisation should consider having its privacy processes assessed periodically by an independent party to identify areas that may need improvement.

Privacy Management Framework – Checklist

This checklist is designed to assist an organisation to implement privacy-enhancing practices and processes, and strengthen the privacy culture of an organisation.

Whether an organisation has implemented or implements all or some of the measures listed will depend on a variety of factors, including the size of the organisation, its functions, the types of information it collects, and its relationship with the public.

This checklist should be completed annually by the organisation's privacy officer and endorsed by the organisation's executive. When completing the checklist, the privacy officer, or privacy team, should comment on how the organisation has implemented the action, or intends to implement the relevant action, and make a robust assessment of the effectiveness of the organisation's practices.

Privacy Management Framework – Organisation Checklist	
Part 1 – Organisational commitment	
Action	*Comment*
The executive and senior management are proactively engaged in building the organisation's privacy culture. *Describe how the executive is engaged or the actions that will be taken to engage the executive in building the organisation's privacy culture.* *For example, privacy compliance is a standing item in executive meetings, reports of privacy complaints and breach trends are shared with the executive.*	
The organisation understands which privacy laws apply to it and the relevant privacy obligations that flow. *Consider if the organisation also has obligations under the Health Records Act 2001 and the Privacy Act 1988 (Cth).*	
Key roles and responsibilities for privacy management including a privacy officer are assigned. *Consider if privacy officer role accountabilities can be included in performance development planning.* *List each role, the person assigned to that role, and the relevant responsibilities of that role.*	

Appropriate resourcing is allocated to maintain organisational privacy expertise. *Evaluate if appropriate resourcing is provided or further resourcing is required.*	
A privacy by design approach is adopted for all initiatives involving personal information. *Detail how this has been achieved, or the actions that will be taken to implement privacy by design.*	
The functions and role of OVIC are understood. *Describe what has been done or actions undertaken to understand OVIC's regulatory role.*	
Part 2 – Privacy practices	
Action	*Comment*
Processes and policies for handling personal information that cover the information lifecycle are maintained. *List all the processes or policies that exist for handling personal information. Outline who is responsible for each item.*	
A privacy policy that is easy to understand and up to date is available to the public. *Detail where the policy can be accessed and what actions have been taken to ensure it is easy to understand.*	
Collection notices are tailored and implemented at each point where personal information is collected. *Consider listing each instance or location where a collection notice is provided.*	
How and when personal information can be shared is understood across the organisation. *Detail the actions taken to ensure staff with access to personal information are aware of their obligations.*	

The practices of contracted service providers are reviewed and align to the organisation's obligations. *Describe how the organisation ensures contracted service providers adhere to relevant privacy protections.*	
A register detailing the organisation's personal information holdings is maintained. *For example, an Information Asset Register.* *Detail where the register is located and who is responsible for maintaining it.*	
Privacy is incorporated into staff inductions and staff training programs. *Describe how privacy is incorporated into inductions and training*	
The organisation identifies privacy risks and adds them to the organisational risk register. *Discuss the organisation's risk management processes in relation to privacy.*	
Security obligations under the Victorian Protective Data Security Framework are known (where applicable). *Detail who is responsible for information security and describe how it is promoted across the organisation.*	
Procedures exist for the disposal of personal information, and destruction when it is no longer required. *Describe what the procedure or policy is, where it is located, and who is responsible.*	
Privacy Impact Assessments are undertaken on all projects and initiatives involving personal information or information management. *Discuss how this has been achieved or what actions are being taken. For example, PIAs are built into project initiation documentation.*	
There is a privacy complaints and enquiries process. *Detail these processes, who is responsible for each, and how the public can access them.*	

There is an established data breach response plan. *Detail where the plan is located and how it has been communicated to the organisation.*	
The organisation understands its obligations under the Incident Notification Scheme (where applicable). *Describe what procedures have been implemented in response to the Incident Notification Scheme.*	
Records of privacy complaints, privacy breaches and reviews of privacy processes are maintained. *Describe the record keeping practices of the organisation and where the relevant records are stored.*	
Whole of organisational awareness activities are undertaken annually. For example, participating in Privacy Awareness Week. *Outline the activities undertaken or how the organisation participates in raising awareness.*	
Part 3 – Monitor, review, and improve	
Action	*Comment*
Privacy policies, collection notices, PIAs and other processes are regularly monitored and reviewed. *Organisations may choose to complete OVIC's privacy policy self-assessment tool.* *List when each policy should be reviewed and who is responsible.*	
Changes to information management processes or practices are implemented based on the findings from reviews. *Outline the changes that were made to the relevant policies or processes.*	
Changes to information management processes or practices are communicated to all relevant staff and stakeholders. *Describe how any changes are communicated across the organisation.*	

Risk registers are actively managed to ensure privacy risks are being managed and appropriately mitigated. *Detail who is responsible for reviewing the risk register and when it should be reviewed.*	
The privacy implications of new technologies are assessed, and privacy policies and collection notices are updated as required. *Detail any new technologies that have been introduced, and if privacy policies, collection notices and PIAs have been updated as a result.*	
Records of privacy complaints, privacy breaches and privacy process reviews are analysed to identify common themes, systemic privacy risks and areas of improvement. *Detail any themes or risks identified and how these have been addressed or the actions taken.*	
An avenue for staff and the public to provide feedback or make a complaint to the organisation's privacy officer or team exists. *Detail how this is provided or the processes that exist.*	
Privacy processes or practices are independently assessed where appropriate to identify areas for improvement. *Detail any processes or practices that have been independently or externally assessed and any outcomes.*	