Office of the Information Commissioner
Queensland

IPOLA

IPOLA GUIDELINE

Applying the legislation – Information Privacy Act 2009

Privacy self-assessment guide

This guide does not reflect the current law.

It highlights important changes to the *Information Privacy Act 2009*.

This guide does not constitute legal advice and is general in nature only. Additional factors may be relevant in specific circumstances. For detailed guidance, legal advice should be sought.

1.0 Overview

This guide is intended to assist agencies to assess their practices, procedures, and activities for compliance with the *Information Privacy Act 2009* (Qld) (**IP Act**) and its Queensland Privacy Principles (the privacy principles).

This guide is not a one size fits all guide which can be applied strictly to every agency. It provides guidance and suggestions, but each agency will have to develop their own self-assessment plan appropriate to their circumstances. Individual business units within the agency may need to further personalise the assessment process.

1.1 Acknowledgements

This guide is based on and draws from the Office of the Victorian Privacy Commissioner's ***Privacy Audit Manual*** and the Office of the Privacy Commissioner of Canada's ***PIPEDA Self-assessment Tool*.**

2.0 Privacy self-assessment

Privacy self-assessment is a tool for agencies to use to evaluate and assess their compliance with the IP Act. The self-assessment may also identify gaps and/or risks in an agency's management of personal information and allow it to improve its privacy systems and practices.

Regular self-assessments can form part of an agency's privacy management systems and demonstrate a responsible privacy management culture.

There are three basic ways in which an agency could conduct a self-assessment:

- individual business units within the agency analyse their personal information management practices and assess their compliance against the IP Act
- another party within the agency, separate from the business unit being analysed, reviews, and assesses the business unit's compliance; or
- one party in the agency, for example the officer or team responsible for IP Act compliance, could assess all of an agency's business units as part of an assessment of the entire agency.

An important part of effective self-assessment involves maintaining accurate records of privacy complaints, including how complaints were dealt with and their outcomes and any breaches of the obligation to comply with the privacy principles. These records should be reviewed as part of any self-assessment exercise to identify:

- common or systemic issues with personal information handling which could lead to a breach of the IP Act
- issues with the privacy complaint handling process; and
- the effectiveness of measures introduced to prevent further breaches.

Where agencies have not maintained specific records of this type, information about privacy complaints could be gathered as part of the assessment process. Three years would provide an objective indication of what agency customers think and where issues of concern may lie.

Self-assessment can be approached in a number of ways, for example:

- conducting a single assessment exercise across the whole agency at one time
- creating a schedule which allows for business units to be assessed on the basis of a risk management approach, first assessing those business units considered to be highest risk then moving to those which are lower risk
- a pilot project could be conducted in one unit, or several smaller units, to assess the effectiveness of the self-assessment, which would allow the approach to be adjusted before moving on to the rest of the agency.

An effective self-assessment process will involve not only reviewing an agency's privacy practices but gathering material to show that the privacy practices are being carried out. For example, if a policy sets out that a specific sort of personal information will only be collected with the consent of the individual, samples of that consent should be examined as part of the assessment process.

Self-assessments should be carefully planned, as they will inevitably involve time and resources, not just of those conducting the assessment but of the business units who will have to divert time from their activities to participate in the review. The fact that the privacy assessment will generally involve additional work for the business unit on a temporary basis should be incorporated into the planning.

Agencies should:

- develop an assessment plan
- conduct a personal information inventory
- conduct a policy and procedure inventory and review; and
- keep and review records of privacy complaints and any privacy breaches.

2.1 Developing an assessment plan

An effective plan will:

- describe the business units of the agency which are to be assessed
- provide a brief description of their responsibilities and activities and the relevant privacy principles against which their personal information practices will be assessed; and
- set out the proposed schedule for the unit's assessment.

A decision will need to be made about what the assessment is going to evaluate. Examples of things which could be assessed are:

- the extent to which the policies and procedures do the job they are intended to do. For example, if a privacy policy is supposed to set out how the agency will comply with QPP 5 , the policy should be evaluated to determine if it does that effectively
- the extent to which the policies and procedures are being implemented effectively. For example, if a security protocol is supposed to limit access to human resources information, access to the information should be tested and past access audited to determine if the control is, in fact, limiting access; and
- whether the controls or policies have been implemented and are operating effectively.

2.2 Conducting a personal information inventory

A privacy assessment will be easier to conduct if each business unit involved in the assessment creates an inventory of the categories of personal information it collects, holds, uses, or discloses. Categories of personal information could be recorded in, for example, a spreadsheet, which describes at a high level the types of personal information, how it is collected, used, disclosed, maintained, and disposed of or archived.

The retention and disposal schedules issued by the Queensland State Archivist may be useful for this process.

The following questions could be useful as a guide when preparing a personal information inventory:

- What personal information does the business unit collect?
- How is it collected and in which situations?
- Why is it collected?
- Who in the agency uses the personal information?

- Who has access to it?
- Where and how is it stored?
- What methods are used to ensure it is secure?
- Is it disclosed outside the agency? If so, to whom and why is it disclosed?
- How long is the personal information kept, and when and how is it disposed of (keeping in mind the obligations under the *Public Records Act 2002* (Qld))?

2.3 Conducting a policy and procedure inventory

This step involves simply making a list of the policies, procedures, standards, or work practices that are relevant to each business unit's management and use of personal information. These may be agency documents, or whole-of-government documents such as Information Standards. Any legislation that affects personal information held by the business unit should be included in this inventory.

2.4 Review privacy complaint and breach records

This step involves reviewing records relating to privacy complaints and privacy breaches. The way the complaints were handled should be assessed, to identify:

- compliance with mandatory notification of data breach (**MNDB**) scheme in chapter 3A of the IP Act,[1] including the obligation to publish a data breach policy and keep a data breach register
- any possible improvements to be made in the privacy complaint handling system used by the agency; and
- areas of common concern among the agency's customers.

Where a complaint identified a privacy breach, or a privacy breach was identified through other means, the measures introduced to contain and mitigate the breach, and/or prevent it reoccurring should be assessed for effectiveness and appropriateness. If the breach has reoccurred, a different approach will need to be identified.

3.0 Assessment planning

Part of the planning process, particularly in large and/or complex agencies, will be deciding which business units are a priority for privacy assessment. There are a number of factors which can affect the prioritisation process, such as strategic planning and level of risk.

3.1 Strategic planning

Most Queensland government agencies have a strategic plan, which is used to set out long term goals and to prioritise agency activities and work. Privacy self-assessments can be linked to, or developed with reference to, the strategic plan, to ensure that the assessment is conducted in accordance with, and contributes to, the agency's priorities.

[1] For more information see ***Mandatory Notification of Data Breach scheme***

3.2 Risk assessment

Business units which pose a higher risk than others should be prioritised. There are a number of factors to be considered when determining which business units of an agency may present a higher risk than others, such as:

- the sensitivity of the personal information held
- the consequences of the breach
- any trends in privacy complaints and enquiries
- issues that are the focus of public attention or concern
- emerging technological issues
- other agency activities which could impact on the assessment, such as the annual budget process or Estimates hearings.

Developing a risk matrix may assist. A risk matrix allows an agency to identify the likelihood and consequences of a business unit being non-compliant with the privacy principles. Appendix One contains a risk matrix based on a matrix tool developed by the Canadian Privacy Commissioner.

3.3 Other factors

Other factors which could affect the prioritisation process are:

- the ease with which a business unit can be assessed, taking into account the level of difficulty, the sensitivity or accessibility of the personal information involved, and the resources that would be required
- the importance of scheduling the assessment process at a time that will not interfere with the activities of the business unit; and
- the extent to which the results of the assessment will assist other business units in privacy compliance, or mean that assessments of some other units will be made simpler or rendered unnecessary.

4.0 Assessment criteria

Criteria are clear and reasonable standards against which the business unit's personal information handling practices can be assessed. These generally take the form of questions because questions make it simpler to reach a conclusion, reduce the level of ambiguity or uncertainty, and help to keep the assessment focused.

The criteria need to be relevant, reliable, neutral, understandable, complete, and appropriate.

The primary source of criteria will generally be the IP Act, particularly the privacy principles, and a list of generic high-level criteria questions are contained in Appendix Two.

Other sources of criteria may be:

- ***guidelines*** produced by the Office of the Information Commissioner
- any relevant public interest approvals

- the agency's privacy and related policies, practices and standards
- previous assessments or audits of the relevant business unit; and
- any relevant legislation.

5.0 Conducting the assessment

To be effective, the assessment process will involve gathering information and material to answer the criteria questions. There are a number of ways to do this.

For example:

- conducting interviews with relevant business unit officers
- circulating hard copy or electronic surveys or questionnaires
- reviewing files and documents; and
- direct observation or physical inspection.

5.1 Types of material

There are generally four types of material considered during the assessment process:

- physical, which may be gathered by, for example, observation of work practices or inspecting an asset (this may not be relevant to all business units)
- documentary, such as reports, correspondence, and audit logs
- verbal, often gathered through the interview process; and
- analytical, which comes from evaluating the other types of material and assessing the degree to which there is support for the conclusions reached in the assessment process.

6.0 Outcome of the assessment

It is good practice to review the outcome of the assessment process with the business unit which was assessed before any report is finalised. Any indication that the unit is not compliant with the privacy principles should be discussed to identify any temporary or mitigating circumstances.

If a business unit cannot demonstrate that it is able to meet the assessment criteria, then it may not be compliant with the IP Act. Evaluating the results of the self-assessment will assist an agency to identify any areas which may be of concern and to take steps to address any privacy compliance issues.

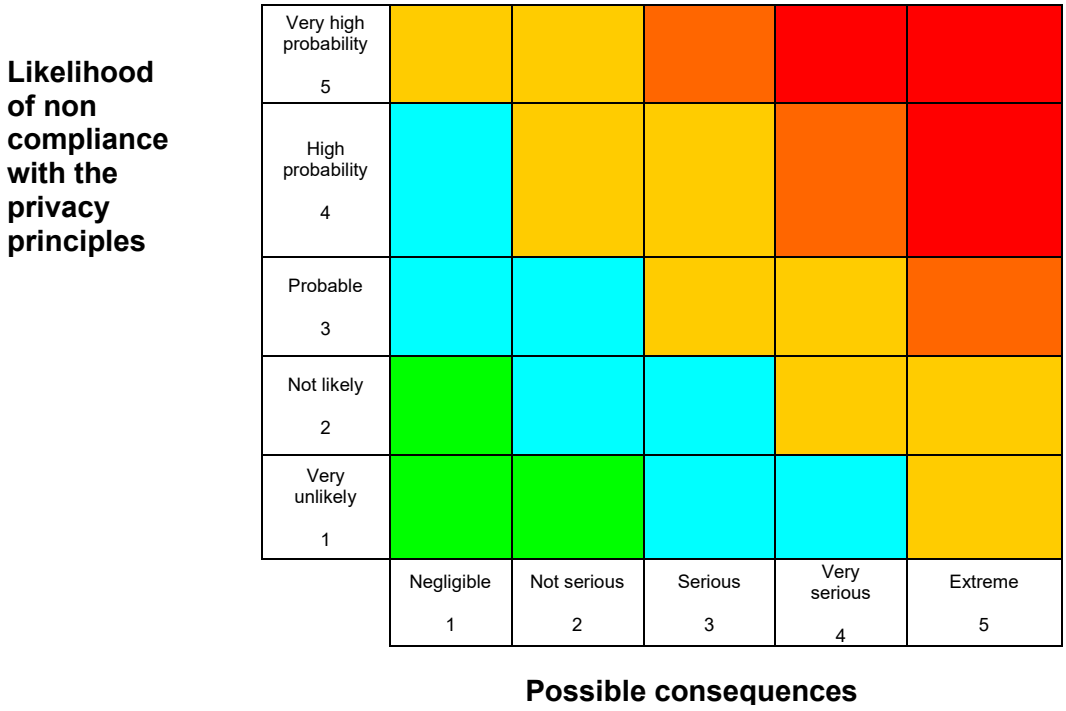
For additional IPOLA assistance, please contact the IPOLA team by email IPOLA.Project@oic.qld.gov.au

For information and assistance on current legislation, please refer to the OIC's guidelines, or contact the Enquiries Service on 07 3234 7373 or by email enquiries@oic.qld.gov.au

Published August 2024 and Last Updated 22 August 2024

Appendix one – Risk matrix

The *PIPEDA Self-assessment tool* developed by the Office of the Privacy Commissioner of Canada contains a risk matrix useful when conducting privacy self-assessments, on which the below is based.



The *likelihood of non-compliance* refers to the chance of an event happening which would not comply with the privacy principles. The *possible consequences* refer to the potential outcome of that event.

Likelihood

Level	Descriptor	Description
5	Very high probability	The event has occurred regularly or often, or will almost definitely occur.
4	High probability	Event has occurred more than once, or has occurred in similar circumstances, or it is highly likely to occur.
3	Probable	Event has previously occurred, or has been observed in similar circumstances, or it may occur.
2	Not likely	Event has occurred infrequently to others in similar circumstances, but it has not occurred previously in the agency and it is not likely to do so.
1	Very unlikely	Event has almost never or never been observed, it may occur only in exceptional circumstances, or it is highly unlikely to occur.

Possible consequences

Level	Descriptor	Description
5	Extreme	The outcome of the event would cause serious, long term damage to an agency and/or significant damage to the person's reputation or finances, or emotional distress.
4	Very serious	The outcome of the event could include significant concerns for an agency and/or significant damage to the person's reputation or finances, or emotional distress.
3	Serious	The outcome could cause problems for an agency but could be managed internally and/or could have moderate impact on the individual, such as the exposure of some financial information and further exposure is limited.
2	Not serious	The outcome might impact on the agency but would be dealt with internally and be of low consequence and/or the impact on the individual could be contained within the agency and further exposure limited.
1	Negligible	The outcome might impact in a minimal way on the agency but could be absorbed through normal agency activity and/or the impact would be of low consequence to the agency and the individual.

Appendix two – Assessment questions

Purpose

An effective self-assessment will involve measuring the practices and procedures of a business unit against set criteria. For a privacy self-assessment, these criteria can be drawn from the privacy principles.

The following checklists may be useful in conducting a privacy self-assessment, but note that they contain very general questions, based on high level principles drawn from QPPs. Agencies should consider developing additional agency or business unit specific questions to assist in conducting the assessment.

Accountability

Criteria question	Assessment			Evidence	Actions
	Met	Not met	Partially met		
Are privacy policies complete and easy to understand?					
Is there someone in the agency who is responsible for agency compliance with or overseeing/managing the IP Act?					
Do privacy policies apply to the information of officers as well as members of the public?					
Have agency officers been given training about their obligations under the IP Act?					
Has the agency met its obligations when entering into contracts involving personal information?					
Have personal information policies been clearly communicated to agency officers?					
Does the agency have procedures in place to ensure new staff are given appropriate training in personal information handling?					
Has the agency developed documentation to explain their personal information policies and procedures to the public?					

Collection

Criteria question	Assessment			Evidence	Actions
	Met	Not met	Partially met		
Does the agency give individuals the option of dealing with the agency anonymously, or via use of pseudonym, where lawful and/or practicable?					
Does the agency identify why it is collecting personal information before it is collected?					
Does the agency provide a QPP 5 collection notice to individuals from whom personal information is being collected?					
Has the agency determined how much and what kind of personal information it needs to collect?					
Is the amount of personal information collected no more than is necessary for the purpose for which it is required?					
Is the agency collecting sensitive information with consent, or otherwise as authorised by IPP 3?					
Is the agency collecting personal information lawfully and fairly?					
Does the agency have steps in place to evaluate unsolicited personal information under QPP 4?					
Does the agency collect only personal information which is relevant to the purpose for which it is being collected?					

Security

Criteria question	Assessment			Evidence	Actions
	Met	Not met	Partially met		
Is the personal information held by the agency protected against unauthorised access, modification, or disclosure?					
Is the personal information held by the agency protected against misuse, interference or loss,?					
Has the agency adopted physical, technical and administrative safeguards to protect personal information?					
Are security safeguards appropriate considering the sensitivity of the personal information?					
Have agency staff been made aware of the importance of protecting personal information?					
Are there processes in place to record access to electronic records?					
Are there processes in place to ensure personal information is disposed of in a way that does not allow unauthorised access?					

Accuracy

Criteria question	Assessment			Evidence	Actions
	Met	Not met	Partially met		
Are there reasonable measures in place to ensure that personal information is accurate, complete, and up to date before it is used or disclosed?					
Are their procedures in place for people to amend their personal information if it is incorrect?					
Are there processes in place to record when and where key personal information was collected, including when it was updated?					

Openness

Criteria question	Assessment			Evidence	Actions
	Met	Not met	Partially met		
Does the agency make information available about its personal information policies and procedures? Does the agency have in place a clearly expressed and publicly-available QPP Privacy Policy, as required under QPP 1?					
Does the agency provide details to the public of the kinds of personal information it collects and holds, and how that information is collected and held?					
Does the agency tell people the purposes for which it collects, uses and discloses their personal information?					
Does the agency tell people how they can access and request correction of their personal information?					
Does the agency advise the community how they make a privacy complaint, and how that complaint will be dealt with?					
Does the agency advice people whether it is likely to disclose their personal information outside Australia, and, if so, which countries?					
Is there a person members of the public can contact about privacy questions?					

Use and disclosure

Criteria question	Assessment			Evidence	Actions
	Met	Not met	Partially met		
Does the agency use information only for the purpose it was collected, unless one of the exceptions in QPP 6 applies?					
Does the agency disclose information only where the person was advised when it was collected or one of the exceptions in QPP 6 apply?					
Does the agency have procedures in place to ensure that use or disclosure of personal information under QPP 6 is noted on the personal information?					

Complaint and Breach Review

Criteria question	Assessment			Evidence	Actions
	Met	Not met	Partially met		
Is there a documented process for managing privacy complaints and privacy breaches, including a data breach policy as required under the MNDB scheme?					
Is this process documented and available to agency officers?					
Is the process, or a version of it, available to the public? Has the data breach policy been published?					
Is the privacy complaint handling process timely and are complainants generally satisfied with the response given?					
Is there a clear process for complaint handlers to inform relevant agency officers when practices that need changing are identified?					
Is there a clear process to action needed changes where complaint handlers have identified issues?					
Have identified reforms to agency processes been successfully implemented?					
Has there been a reoccurrence of any privacy breaches?					