Office of the Information Commissioner
Queensland

IPOLA

IPOLA GUIDELINE

Interpreting the legislation – Information Privacy Act 2009

QPP 3&6 – Law enforcement agencies & activities

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

All Queensland government agencies[1] must handle personal information in accordance with the Queensland Privacy Principles (QPPs) in the *Information Privacy Act 2009* (Qld) (IP Act).

This guideline is based on and includes material from the Australian Privacy Principle guidelines developed by the Office of the Australian Information Commissioner.

1.1 What is personal information?

Section 12 of the IP Act provides that personal information means information or an opinion about an identified individual or an individual who is reasonably identifiable from the information or opinion, whether the information is true or recorded in a material form.

The individual does not need to be directly identified in the information for it to be personal information. It is sufficient if they can reasonably be identified by reference to other information.

Sensitive information is a category of personal information defined in schedule 5 of the IP Act, and includes information about an individual's racial or ethnic origin, political opinions, religious beliefs, sexual orientation and criminal record. It also includes health, genetic and some biometric information.

Refer to ***Key privacy concepts – sensitive and personal information*** for more information.

[1] References to an agency in this guideline include a Minister, bound contracted service provider, or other entity required to comply with the QPPs.

2.0 Collection of sensitive information

An agency must not collect sensitive information without consent unless one of the exceptions in QPP 3.4 apply.

Under QPP 3.4(d), a law enforcement agency can collect sensitive information without consent if it reasonably believes that collection is reasonably necessary for, or directly related to, one or more of its functions or activities.

This exception is discussed in further detail below. Otherwise, refer to ***QPP 3 – collection of personal information*** for more information.

3.0 Use or disclosure

An agency can use or disclose personal information for the reason it was collected (the primary purpose). An agency can only use or disclose personal information for a secondary purpose as set out in QPP 6.

Use and disclosure are both defined in the IP Act.[2] Refer to ***Key privacy concepts – use and disclosure*** for more information.

Under QPP 6.2(e), an agency can use or disclose personal information for a secondary purpose if the agency reasonably believes that the use or disclosure is reasonably necessary for one or more enforcement-related activities conducted by a law enforcement agency.

If personal information is used or disclosed under QPP 6.2(e), QPP 6.5 requires the agency to make a written note of the use or disclosure. This exception is discussed in further detail below.

4.0 Law enforcement agency and enforcement-related activity

'Law enforcement agency' and 'enforcement-related activity' are defined in schedule 5 of the IP Act. This guideline should be read in conjunction with ***Key privacy concepts – enforcement agencies and enforcement activities*** *(guideline under development)*, which explains these in detail. In summary terms, schedule 5 defines 'law enforcement agencies' to include the Queensland Police Service (QPS), the Crime and Corruption Commission, and other agencies, including agencies to the extent they have responsibility for carrying out certain functions or activities.

4.1 Use or disclosure for enforcement-related activities

QPP 6.2(e) allows use and disclosure by a law enforcement agency for one of its enforcement-related activities. It also allows use and disclosure by a non-law enforcement agency, if the non-law enforcement agency reasonably believes the

[2] Section 23 of the IP Act.

use or disclosure is reasonably necessary for an enforcement-related activity being conducted by a law enforcement agency. The phrases 'reasonably believe' and 'reasonably necessary' are discussed at 5.0 below.

For agencies whose primary function is law enforcement, such as the QPS, not every activity they carry out will be an enforcement-related activity. Human resources, general administration, budgeting, and finance, for example, will not comprise enforcement-related activities merely because those activities are being carried out by a law enforcement agency.

Similarly, agencies which have specific law enforcement functions in addition to other functions, such as local government authorities, can only rely on the law enforcement exceptions for enforcement activity that is related to those specific law enforcement functions.

Other non-law enforcement agencies considering disclosure of personal information to a law enforcement agency under this exception can only disclose personal information to the law enforcement agency if the non-law enforcement agency reasonably believes that disclosure is reasonably necessary for one or more of the law enforcement agency's enforcement-related activities.

For example, if the Department of Water Quality was investigating a possible breach by a local farmer of a breach of the *Clean Water Act 2007* it could disclose personal information about the farmer, for example that he was being investigated, to the local council, neighbours, or farmhands, if the disclosure was a necessary part of the Department's investigation.

4.2 Collection of sensitive information by law enforcement agencies

As noted, under QPP 3.4(d) a law enforcement agency can collect sensitive information without consent if the law enforcement agency reasonably believes that the collection is reasonably necessary for, or directly related to, one or more of its functions or activities

Importantly, QPP 3.4(d) ***only*** applies to the collection ***by*** law enforcement agencies of sensitive information. Agencies which are not a law enforcement agency cannot rely on this exception to collect sensitive information without consent *for* a law enforcement agency. Agencies considering relying on QPP 3.4(d) should therefore consult the definition of law enforcement agency set out in schedule 5 of the IP Act, and satisfy themselves that they comprise a law enforcement agency.

Directly related to a function or activity

Collection of sensitive information will be directly related to a law enforcement agency's functions or activities where there is a close connection or association between the sensitive information and the function or activity. For more information on the meaning of 'directly related to' see **QPP 6 – Use or Disclosure** (guideline under development).

The law enforcement agency must also 'reasonably believe' the collection of sensitive information is directly related – this concept is discussed further below.

5.0 Reasonably believes and reasonably necessary

Central to the law enforcement exceptions are the concepts '***reasonably believes'*** and ***'reasonably necessary'***. As noted above, a law enforcement agency can only collect sensitive personal information where it reasonably believes collection is reasonably necessary for, or directly related to, relevant purposes.

Similarly, agencies must reasonably believe that use or disclosure is reasonably necessary for enforcement-related activities conducted by a law enforcement agency.

Reasonably believes

The phrase 'reasonably believes' imposes an objective test, having regard to how a reasonable person, properly informed, would be expected to act in the circumstances. An agency must have a reasonable basis for the belief, and not merely a genuine or subjective belief. An agency will be responsible for establishing it holds a reasonable belief.

Reasonably necessary

Whether collection, use or disclosure is reasonably necessary is also an objective test: would a reasonable person who is properly informed of all the circumstances view the collection, use or disclosure as necessary? It will be up to the agency to justify the collection, use or disclosure.

Generally, the agency must:

- be satisfied that there is a link between the proposed collection, use or disclosure and the activities; and
- establish that the link is sufficient to make the collection, use or disclosure of information reasonably necessary.

The information does not need to be essential or critical to the activity, but it must be more than just helpful, desirable or expedient.

It is important to take a practical approach when making this determination. If an agency cannot in practice effectively pursue or perform a function without collecting, using, or disclosing information, collection, use or disclosure will generally be considered reasonably necessary for that function or activity.

However, if there are reasonable alternatives available, for example, if deidentified information would be sufficient for the function or activity, it will be more difficult to establish reasonable necessity.

Agencies cannot solely rely on normal business practice in assessing whether collection, use or disclosure of personal information is reasonably necessary. The primary consideration is whether, in the specific circumstances, the collection, use or disclosure is reasonably necessary.

Example – gathering intelligence

Investigators from a law enforcement agency suspect a building is being used to hold illegally smuggled wildlife and they ask an agency to disclose the personal information of individuals associated with the building.

Even though the investigators do not know to what extent, if any, those individuals are involved in the smuggling operation, the disclosure would still be reasonably necessary, because it forms an important part of the law enforcement agency's intelligence gathering about the suspected smuggling.

When deciding whether to use or disclose personal information to another entity, or use it by transferring it to another part of the agency, relevant considerations include:

- the reason for the request – the requesting officer or agency should establish what is being investigated, at least in broad terms, and why the information is necessary
- for disclosure—whether it is more appropriate, given the amount and sensitivity of the personal information, to require a warrant or other legal authority to be produced.

It is also good practice to for an agency, before disclosing personal information, to establish whether the requesting officer has been identified as a legitimate officer, and has provided their details, including work unit and supervisor and that the investigation is legitimate, especially where the request involves a large amount of personal information or personal information of a sensitive nature.

The enforcement-related activity does not necessarily need to have started. The information may, for example, be reasonably necessary for the law enforcement agency to start an investigation.

Agencies should ensure they only collect, use, or disclose the minimum amount of information needed by the law enforcement agency. For example, the agency may hold a range of personal information about an individual, such as their contact details, photo, and information about their education. The agency must consider whether all of this information is reasonably necessary and, if not, remove the unnecessary information before using or disclosing it.

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 01 August 2024