Office of the Information Commissioner
Queensland

IPOLA

IPOLA GUIDELINE
Interpreting the legislation – Information Privacy Act 2009

QPP 11 – Security, deidentification and destruction of personal information

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.

Overview

All Queensland government agencies[1] must handle personal information in accordance with the Queensland Privacy Principles (QPP) 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.

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, whether or not it is true or recorded in a material format.

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.

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

QPP 11

Under QPP 11, agencies must take reasonable steps to protect the personal information they hold from misuse, interference, and loss, and from unauthorised access, modification or disclosure.

[1] In this guideline agency includes a Minister.

QPP 11 also requires agencies to destroy or deidentify personal information once it is no longer needed for any purpose for which it could be used or disclosed under the QPPs. This obligation is subject to the provisions of the *Public Records Act 2023* (Qld) and/or any order of a court or tribunal requiring the agency to retain the information.

Security of personal information

The six things QPP 11 requires an agency to take reasonable steps to protect personal information from are: misuse, interference, loss, unauthorised access, unauthorised modification, and unauthorised disclosure of personal information.

These terms are not defined in the IP Act and their meanings often overlap.

Misuse

An agency misuses personal information if it is uses it for a purpose not permitted by the IP Act. Use is defined in section 23 of the IP Act and QPP 6 sets out when an agency can use personal information.

See ***Key privacy concepts – Use and disclosure*** and the ***QPP 6 guidelines*** (under development) for more information.

Interference

Interference with personal information occurs if there is an attack on personal information held by an agency that interferes with the personal information but does not necessarily modify its content.

Interference includes an attack on a computer system that, for example, leads to exposure of personal information.

Loss

Loss of personal information covers the accidental or inadvertent loss of personal information held by an agency. This includes:

- physically losing personal information, including hard copy documents, computer equipment or portable storage devices containing personal information, by, for example, leaving it in a public place
- electronically losing personal information, by, for example, failing to keep adequate backups of personal information in the event of a systems failure.

Loss can also occur as a result of theft following unauthorised access, unauthorised modification, or as a result of power outages or natural disasters such as floods or fires.

It does not apply to the intentional destruction or deidentification of personal information done in accordance with the QPPs or the *Public Records Act 2023* (Qld).

Unauthorised access

Unauthorised access of personal information occurs when personal information is accessed by someone who is not permitted to do so. This includes unauthorised access by an employee of the entity or independent contractor, as well as unauthorised access by an external third party, e.g., via malware or hacking.

Unauthorised modification

Unauthorised modification of personal information occurs when personal information is altered by someone who is not permitted to do so, or is altered in a way that is not permitted under the IP Act.

Unauthorised modification can occur as a result of, for example, unauthorised alteration by an employee, or following unauthorised access to databases by an external third party.

Unauthorised disclosure

Disclosure is defined in section 23 of the IP Act. Unauthorised disclosure occurs when an agency:

- makes personal information accessible or visible to others outside the entity, and
- releases that information from its effective control in a way that is not permitted by the IP Act.

This includes unauthorised disclosure by an employee of the agency.

See ***Key privacy concepts – Use and disclosure*** and the ***QPP 6 guidelines*** (under development) for more information on permitted disclosures.

Reasonable steps

As part of taking reasonable steps to protect personal information, an agency should consider how it will protect personal information at all stages of the information lifecycle. This includes before personal information is collected (including whether it *should* be collected), once it is collected and held, and when it is destroyed or deidentified once it is no longer needed.

The reasonable steps an agency must take to ensure the security of personal information will depend on the circumstances, for example:

- the amount and sensitivity of the personal information held. Generally, as the amount and/or sensitivity of personal information increases, so do the steps it is reasonable for an agency to take to protect it. Additional measures may be needed to protect sensitive information.[2]
- the possible adverse consequences for an individual if there is a breach. More rigorous steps may be required as the risk of adversity increases.
- the practical implications of implementing the security measure, including time and cost involved. However, the fact that it would be

[2] As defined in schedule 5 of the IP Act.

inconvenient, time-consuming or impose some cost is not enough to make the steps unreasonable. Whether these factors make it unreasonable to take particular steps will depend on whether the burden is excessive in all the circumstances.
- whether a particular security measure is privacy invasive. For example, while agencies must ensure an individual is authorised to access information, they should not require an individual to supply more than the minimum information necessary to identify themselves.

Reasonable steps should include, where relevant, taking steps and implementing strategies in relation to:

- governance, culture and training
- internal practices, procedures and systems
- ICT security
- access security, including audit trails
- third party providers (including cloud computing)
- data breaches
- physical security
- destruction and de-identification; and
- complying with relevant information Standards.[3]

See the ***Securing personal information*** (document under development) for more information.

Destruction or deidentification of personal information

QPP 11 requires agencies to destroy or deidentify personal information that is no longer needed for any purpose.

Limitations – Public records, Australian law, and court orders

Generally, agency documents can only be destroyed or altered if the *Public Records Act 2023* (Qld) and any Retention and Disposal Schedule issued under that Act authorises it.

Agencies must also comply with any other Australian law, or any court or tribunal order, that requires information or documents to be kept in an unaltered form.

As such, the obligation in QPP 11 to take reasonable steps to destroy or deidentify personal information will not apply to personal information that:

- must be retained unaltered as a public record
- must be retained unaltered by any Australian law; or
- a court or tribunal has ordered must be retained.

[3] Queensland Government Information Standard 18, Information Security, contains 10 mandatory information security principles and requires all departments and agencies to establish an appropriate information security culture.

No longer needed for any purpose

QPP 11 specifies that the personal information must no longer be needed for any purpose for which the information could be used or disclosed under the QPPs.

This means that the purpose for which it is retained in an identified form can be either the primary purpose of collection or any other secondary purpose set out in QPP 6.

However, similar to the principles governing collection of information, there must be a genuine expectation of required future use or disclosure. This means agencies must actively consider whether the personal information will actually be required for a permitted purpose. Retaining information 'just in case' it may be needed for some future use by the agency or a third party is not sufficient.

Information will often have statistical and research value and can inform and guide public policy decisions, but the purpose for which personal information is being kept must be specific and identifiable, rather than undefined and hypothetical.

Reasonable steps to deidentify or destroy

QPP 11 requires agencies to take reasonable steps to ensure that personal information is deidentified or destroyed when it is no longer needed for a permitted purpose.

Reasonable steps

What constitutes reasonable steps to deidentify or destroy personal information depends on the specific circumstances, for example.

- the amount and sensitivity of the personal information — more rigorous steps may be required as the quantity of personal information increases, or if the information is sensitive information.[4]
- the nature of the agency. Relevant considerations include the agency's size, resources and information storage methods. For example, the reasonable steps expected of an agency that operates off a single information management system may differ from the reasonable steps required of an agency with a decentralised model.
- the possible adverse consequences for an individual if their personal information is not destroyed or de-identified — more rigorous steps may be required as the risk of adversity increases.
- the agency's information handling practices, such as how it collects, uses and stores personal information, including whether personal information handling practices are outsourced to third parties.
- the practicability, including time and cost involved – however, the fact that destroying or de-identifying personal information would be inconvenient, time-consuming or impose a cost does not automatically make it unreasonable for an agency to do so. Whether these factors make it unreasonable to take a particular step will depend on whether the burden is excessive in all the circumstances.

[4] As defined in schedule 5 of the IP Act.

See ***QPP 3 and QPP 6 guidelines*** (under development) for more information.

Deidentification

De-identification involves removing or altering personal information. Generally, deidentification includes two steps:

- removing personal identifiers, such as an individual's name, address, date of birth or other identifying information; and
- removing or altering other information that may allow an individual to be identified, for example, because of a rare characteristic of the individual, or a combination of unique or remarkable characteristics that enable identification.

Personal information is deidentified when the identity of the individual the information is about cannot, and in the future will not, be reasonably ascertainable.[5] Deidentification must be permanent, which means that the agency must not be able to match the deidentified information with other records to re-establish the individual's identity.

Deidentification may be more appropriate than destruction if the deidentified information could provide further value or utility to the agency or a third party. For example, if:

- the agency shares deidentified information with researchers, or
- the agency uses deidentified information to develop or inform public policy.

Whatever deidentification method is used, the risk of reidentification must be actively assessed and managed to mitigate this risk. If the risk of reidentification cannot be appropriately minimised, the agency should consider taking reasonable steps to destroy the personal information.

Where personal information is stored on third party hardware, e.g., cloud storage, and the agency tells the third party to deidentify the personal information, taking reasonable steps includes verifying that it was done.

See ***Providing access to Documents*** (guideline under development) for more information.

Destruction

Personal information is destroyed if it can no longer be retrieved. The reasonable steps an agency takes to destroy personal information depends on whether the personal information is held in hard copy or electronic form.

For hard copy personal information, throwing it in the garbage or recycling would generally not constitute taking reasonable steps to destroy the personal information, unless it had already been destroyed through a process such as pulping, burning, pulverising, disintegrating or shredding.

[5] As per the definition of personal information in section 12 of the IP Act.

For personal information in electronic form, reasonable steps will vary depending on the kind of hardware used to store the personal information. In some cases, it may be possible to 'sanitise' the hardware to completely remove stored personal information. If hardware cannot be sanitised, reasonable steps must be taken to destroy the personal information in another way, such as by irretrievably destroying it.

Where it is not possible to irretrievably destroy personal information held in electronic format, an agency should consider taking reasonable steps to deidentify the personal information. Alternatively, the agency could put the information beyond use as set out below.

If personal information is stored on third party hardware, eg cloud storage, and the agency tells the third party to destroy it, taking reasonable steps includes verifying that it was done.

Putting personal information beyond use

If an agency cannot irretrievably destroy personal information held in electronic format, reasonable steps to destroy it would include putting the personal information 'beyond use'.

Personal information is beyond use if it is no longer available for use in the ordinary performance of the agency's functions. The agency must:

- not be able, and will not attempt, to use or disclose the personal information
- not be able to give any other entity access to the personal information
- apply appropriate technical, physical and organisational security to the information, including, at a minimum, access controls including logs and audit trails, and
- commit to taking reasonable steps to irretrievably destroy the personal information if or when this becomes possible.

Limited application of beyond use

The circumstances in which an agency could not destroy electronic personal information will be very limited, e.g., if it is impossible to irretrievably destroy the personal information without also irretrievably destroying other information the entity is required to retain.

Office of the Information Commissioner
Queensland

IPOLA

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 1 August 2024