Office of the Information Commissioner
Queensland

IPOLA

IPOLA GUIDELINE

Applying the legislation – Information Privacy Act 2009

Data Analytics

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

Queensland government agencies[1] must comply with the Queensland Privacy principles (**QPPs**) in the *Information Privacy Act 2009* (Qld) (**IP Act**) when dealing with personal information.

1.1 What is personal information?

Personal information is information about an individual who can be identified or is reasonably identifiable from the information or opinion, whether it is true and whether it is recorded in a material form. Companies do not have personal information and neither do deceased people.

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

1.2 What is data analytics?

Data analytics is the process of examining data sets in order to draw conclusions about the information they contain. It involves processes that include analysing existing datasets and extracting new insights into various patterns, relations, and connections.

When an agency wants to use data analytics on data that includes personal information, regardless of whether that personal information was collected by the agency or not, there can be significant privacy challenges.

[1] Agency includes a Minister, bound contracted service provider or other entity subject to the IP Act.

2.0 Should I use de-identified data?

The privacy principles only apply to personal information, which is information that can be linked to an identifiable individual. If the information can be de-identified, or broken down into aggregated unidentified data, such as statistics, then it will no longer be personal information and the privacy principles will not apply.

Agencies considering data analytics projects that use data containing personal information may want to consider whether de-identified data could be used. De-identifying personal information enables it to be used, shared, or made publicly available without the agency having to consider compliance with the privacy principles.

It is important to note that de-identification is a risk-management exercise, not an exact science. De-identified datasets always carry the risk of re-identification. Datasets that don't contain obvious personal information could be linked with additional datasets or be the subject of further deeper analysis from which re-identification of personal information could occur.

It is recommended that agencies seek specialist expertise when undertaking a de-identification exercise, particularly if the de-identified information is to be made public.

Refer to ***Privacy and de-Identification*** (guideline under development) for more information.

For some data analytics activities, however, de-identified data may not be suitable. Where datasets contain personal information, agencies must comply with the privacy principles.

3.0 Using and disclosing personal information

QPP 6 governs the use and disclosure of personal information. QPP 6.2(g) allows agencies to use or disclose personal information for research or the compilation or analysis of statistics in the public interest.

Additionally, under QPP 6.2 and schedule 4, part 2 of the IP Act, health agencies can use health information without the consent of the individual for research, or the compilation or analysis of statistics, relevant to public health or public safety.

QPP 6 also allows personal information to be used or disclosed with consent or for a directly related or related purpose that the individual would expect.

Limits of authority

The IP Act operates subject to the provisions of other Acts relating to the use or disclosure of personal information, such as the *Child Protection Act 1999* or the *Hospital and Health Boards Act 2011*. The QPPs do not override legislation that prohibits use or disclosure.

An agency intending to use or disclose data containing personal information must consider whether there are any legislative provisions that would impact or prohibit the use or disclosure.

Refer to ***QPP 6 – use or disclosure***, ***Key privacy concepts, use and disclosure*** and ***QPP 3&6 – Health agencies: collection, use or disclosure of health information*** for more information on applying these QPPs.

3.1 Do I need to let people know about the data analytics activities?

QPP 5 requires an agency which collects personal information to take reasonable steps to inform the individual of the relevant matters listed in QPP 5.2. QPP 5 applies regardless of how the agency acquired the information, i.e., directly from the individual or from a third party.

If the agency knows when it collects personal information that it may use it for data analytics, it should include that purpose in the QPP 5 matters, however this purpose should not be included as a matter of course.

Refer to ***QPP 5 – what agencies must tell people when collecting personal information*** for more information.

3.2 What if I want to outsource data analytic activities?

If an agency is considering outsourcing data analytics activities that involve personal information, it must take all reasonable steps to ensure the contracted service provider is bound to comply with the privacy principles.

If the contracting agency does not take all reasonable steps to bind the contracted service provider, the contracting agency will be responsible for any breach of privacy arising from the actions of the contracted service provider.

For more information refer to ***Binding a contractor to the IP Act*** (guideline under development).

4.0 Security of personal information

QPP 11 requires agencies to protect personal information from misuse, interference, loss, and from unauthorised access, modification or disclosure. In most cases, agencies will already have safeguards in place to appropriately protect the personal information they hold. The same security considerations should apply to analytical data that may be a variation on the personal information already held by the agency.

Access to agency personal information holdings for data analytics purposes should be limited both to those who have a business need to do so, and to the specific information required.

4.1 Can I use cloud services for data analytic activities?

In some cases, agencies may consider carrying out data analytics using cloud services. Refer to ***Cloud computing and the privacy principles*** (guideline under development) for guidance.

5.0 Privacy by Design

Privacy by design is an approach that builds privacy up front into the design specifications and architecture of new technologies and business processes. It makes privacy an integral component of the functions being delivered.

A privacy impact assessment (**PIA**) is an assessment tool that can map the data flows involved in a project to make sure that data can be collected, used, processed, stored and shared in a manner in line with an agency's privacy principle obligations.

If there are any conditions that need to be met or safeguards to be put into place, a PIA can help identify them and ensure the necessary measures are adopted in the project plan.

A PIA can also clearly identify the benefits associated with a data project so that risk mitigation measures can be evaluated with the benefits of the project in mind.

Some key questions a PIA can consider include:

- Does the project involve any new or changed ways of handling personal information?
- Is the project likely to have a significant impact on individuals?
- Does the project involve datasets that have been matched or combined, for example involving data from different projects set up for different purposes?
- Is the project likely to be perceived as privacy intrusive?

As the objectives and purpose of the data analytics project shift, new privacy considerations may emerge. Agencies will need to continue to review the PIA to ensure the privacy solutions are working as expected, and how emerging risks will be addressed.

For more information, refer to ***Privacy Impact Assessments*** (IPOLA resources under development).

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 20 August 2024