Office of the Information Commissioner
Queensland

IPOLA

IPOLA GUIDELINE

Applying the legislation – *Information Privacy Act 2009*

MNDB scheme
Data breaches and contracted service providers

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. Mandatory Notification of Data Breach scheme

Agencies are required to deal with personal information in compliance with the *Information Privacy Act 2009* (Qld) (**IP Act**).[1] Chapter 3A of the IP Act creates a mandatory notification of data breach (**MNDB**) scheme.

The MNDB scheme requires agencies[2] (other than local government[3] which will be subject to the MNDB scheme from 1 July 2026) to notify the Information Commissioner and certain individuals of eligible data breaches. Generally, the obligations under the MNDB scheme do not apply to service providers contracted to provide services to or on behalf of government.[4] However, there may be circumstances where data breaches involving personal information in the possession of a contracted service provider will also be considered to be a data breach of an agency.

If such a data breach is likely to result in serious harm to an individual to whom the personal information relates, this will be considered as an eligible data breach of the agency. This guideline is designed to assist Queensland government agencies to understand how this may apply and to identify whether breaches involving contracted service providers will impose obligations on agencies under

[1] All references to legislation in this document refer to a section of the *Information Privacy Act* 2009, unless otherwise stated.
[2] In this guideline, agency includes a Minister but does not include a local government.
[3] Application of the MNDB scheme to local governments is delayed until 1 July 2026. Local government should refer to *Responding to a potential privacy breach, and Privacy breach management and notification*.
[4] Agencies remain, however, obliged to take reasonable steps to ensure contracted service providers are required to comply with privacy principle requirements, in accordance with Chapter 2, Part 4 of the IP Act.

the MNDB scheme. More detailed information regarding the MNDB scheme can be found in the ***Mandatory Notification of Data Breach***, guideline.

2. Personal information 'held' by an agency

The obligations under the MNDB scheme apply to personal information held by an agency.[5]

Section 13 defines "held or holds" in relation to personal information as:

> *Personal information is held by a relevant entity, or the entity holds personal information, if the personal information is contained in a document in the possession, or under the control, of the relevant entity.*

Examples of physical possession include documents stored in an agency's records management or IT systems, and hard copy documents on a 'paper' file or in a physical storage repository.

The inclusion of the words "under the control" in the definition expands the ordinary meaning of the terms 'hold or held' to include situations where an agency may not be in physical possession of the relevant document containing personal information, but it still retains a legal entitlement to possession or a right to deal with the information. This could include documents held by a contracted service provider.

2.1. Identifying when information in the possession of a service provider is "held" by an agency

Agencies will be in 'control' of a document where they have a present legal entitlement to physical possession,[6] or a power to handle the information, such as by way of a contractual or other legal right. This may include, for example, documents provided to a legal services provider by an agency for the purposes of seeking advice,[7] or documents an agency may require a service provider to provide to the agency under the terms of a service agreement.

When a data breach occurs which involves information in the possession of a contracted service provider, agencies will need to consider whether the information is "held" by the agency. This will require consideration of the specific set of circumstances, including factors such as:

- The right of the agency to control the use of the information, including to be provided with the information by the service provider
- Reasons why the information was collected or created
- Who created or collected the information, and

[5] Other than personal information in a document to which the privacy principles do not apply.
[6] *Y46 and Queensland Police Service* [2020] QICmr 3 (4 February 2020), [44]; *Price and Nominal Defendant* (1999) 5 QAR 80, [18].
[7] For more information on this point, see OIC's guideline Documents held by third party legal providers. While this guideline concerns information access applications made under the RTI Act, the applicable statutory tests and legal principles are substantially similar.

- The contractual arrangements governing the service provision, including whether the contractual terms cover issues such as:
    - rights to access and use the information, including the purposes of the use
    - when information can be disclosed and to who
    - any rights of the service provider to use and disclose the information
    - penalties or outcomes in the event of the service provider mishandling the information
    - ownership or rights to the information on completion of the service contract, and
    - any indemnity for claims against the agency for claims arising from actions of the service provider.

Example of arrangement where personal information in the possession of a service provider will be considered as held by the agency

An agency enters into a contract with a service provider for the provision of services to the public. Under this agreement, the service provider is obliged to provide an online customer portal which allows customers of the agency to lodge requests for service and to make payment for agency services. These actions involve the collection and use of personal information. The contract has specific terms which outline that the agency maintains control over this personal information, and there are no clauses in the contract which allow the service provider to use or keep personal information for any purposes other than to fulfill obligations under the contract. The service provider has no other contract or business which involves collection or use of personal information of agency customers.

Where a data breach of the service provider involving unauthorised access to personal information of agency customers occurs, the contractual terms regarding agency control of the information are sufficient to meet the section 13 definition of held or holds as the information is “under the control” of the agency.

Example of arrangement where personal information in the possession of a service provider will NOT be considered as held by the agency

The above contract is altered to allow the service provider to use some of the collected personal information for a purpose not connected to the service agreement with the agency. The service provider uses this information for the purposes of market research where the relevant customers have given their permission. The market research has no connection to the agency, and the information being used for these market research activities is not governed by the service contact.

When the service provider uses the information for its market research activities, it creates a new record containing names and contact details. Although this information was originally collected for the purposes of the contract with the agency, only the service provider has possession or control of this new record.

Where a data breach occurs involving the service provider and this new record, the circumstances will not meet the definition of held or hold regarding the personal information, as the agency is not in possession of the information and has no control over the information.

3. Service provider contracts

Agencies may utilise contracted service providers for both the provision of services to the agency, and for services to the public on the agency's behalf.

3.1. Provision of services to an agency

Agencies often engage service providers to supply externally provisioned ICT services, which can involve agency personal information being hosted on service provider ICT systems. This includes through externally provisioned managed services such as:

- Email or case management systems
- ICT services or functions - eg as application, network or server management
- Application or web hosting
- managed capacity for the provisioning of ICT assets, or
- combinations of the above.

There are also cloud services, such as:

- software as-a-service, e.g. social media, on-line collaboration
- platform or infrastructure as-a-service
- infrastructure as-a-service
- business process or customer relationship management as-a-service
- identity as-a-service. and
- storage as-a-service.[8]

Agencies ordinarily retain high levels of control over information under these types of arrangements. It is common that they will retain a sole right to control the information, and consequently will be considered to hold any relevant personal information in these circumstances for the purposes of the MNDB scheme.

[8] For more information on ICT Service contracts, see Queensland Government, Queensland Government Enterprise Architecture, *ICT as a Service Policy*, ICT-as-a-service policy | For government | Queensland Government.

3.2. Provision of services to the public

It is also common for agencies to contract with private entities to provide services to the public. A common example of this type of arrangement involves the private entity providing a customer portal which enables customers to manage their relationship with the agency, through actions such as making enquiries or lodging online complaints or requests. Determining if an agency holds or held information collected or used by the service provider in these circumstances will be dependent on the circumstances specific to that arrangement, including the contractual terms governing the process. Agencies should ensure the issue of control of information is considered when forming new contracts for service. It is also recommended that existing contracts are reviewed to reach clarity on this issue before it becomes a question which must be considered while responding to a breach.

3.3. Multiple contracts

The provision of services can sometime involve multiple contracts. This can occur when an agency enters into an arrangement with a service provider, and this provider then sub-contracts parts or all of the service provision to another entity. This could be in regard to specific actions under the agreement or it could involve the provision of ICT services under the agreement. Determining whether an agency holds or held information in these circumstances will require detailed analysis of each contract. Agencies will need to be aware of how contracts in the chain interact, how the collection and use of personal information is considered, and which parties have control of the information at different stages of the contractual process.

3.4. Contractual terms

When entering into new, or reviewing existing contracts, agencies should consider the circumstances specific to the type of personal information held. They should also consider the relevant operating environment, and how these factors should influence contractual arrangements regarding handling and use of personal information. It is recommended that agencies consider including specific clauses in contracts, including;

- obligations to promptly report data breaches
- a requirement to contain and mitigate in response to data breaches, and
- a requirement to assist and cooperate with data breach assessments.

When reviewing contracts, agencies should consider if the existing terms will address these points and seek amendment or modification to contractual terms where appropriate.

4. Service providers and the Commonwealth notifiable data breach scheme

Some private sector entities may be subject to the Commonwealth Notifiable Data Breach scheme and other obligations under the *Commonwealth Privacy Act*

1988. However, there is an exemption under section 7B(5) of that Act that applies to acts done or practices engaged in by a contracted service provider to meet the obligations of a State contract. Agencies need to be aware of this exemption and how it may apply to specific contractual arrangements they have, as it is possible that service providers will not be subject to Commonwealth Privacy obligations when performing services under a State contract.

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 January 2025 and Last Updated December 2024