Fact Sheet January 2023

Data breaches and contracted service providers

Who is this information for?	NSW public sector agencies
Why is this information important to them?	This fact sheet will assist agencies to determine whether a data breach involving a contracted service provider is an eligible data breach under the Mandatory Notification of Data Breach Scheme.

The Mandatory Notification of Data Breach Scheme established under Part 6A of the *Privacy and Personal Information Protection Act 1998* (PPIP Act) applies to NSW public sector agencies. Under the Scheme, agencies are required to make notifications to the Privacy Commissioner and affected individuals in the event of an eligible data breach.

The MNDB Scheme does not generally apply to contracted service providers providing services to or on behalf of government. This is because personal information held by a contracted service provider is usually 'held' by the service provider and not by a public sector agency.

However, there are some circumstances where personal information in the hands of a contracted service provider will be "held" by the agency. In those circumstances an agency will have notification obligations under the MNDB Scheme in relation to a data breach involving a contracted service provider.

When is information held by an agency?

Under section 59C of the PPIP Act, an agency is taken to 'hold' personal information for the purposes of the MNDB Scheme if:

1. the agency is in possession or control of the information, or
2. the information is contained in a state record in respect of which the agency is responsible under the *State Records Act 1998* (NSW).

In the context of contracted service providers, it is the first of these two tests which will be relevant.

What does it mean to be in "possession" or "control" of personal information?

An agency will be in possession or control of personal information if the agency:

- has **physical possession** of the information - for example, where information is stored:
  - in an agency's information management system,
  - on a shared drive, or
  - in a hard copy file; **or**

- has a **legal or practical power** to control how the information is dealt with - for example, a contractual or legal right to:
  - access and use information in the hands of a service provider, or
  - require a service provider to provide a copy of the information to the agency.

When will information in the hands of a service provider be "held" by an agency?

Information in the hands of a contracted service provider will be considered to be held by the agency if one of the tests outlined above is satisifed.

Whether an agency is in possession or control of information will depend on the specific facts and circumstances in each instance. Factors that an agency should consider will include:

- whether the agency physically possesses the information or has an intention to possess the information
- whether the agency has a right to control how the information is used or request a copy of the information from a contracted service provider
- the purpose for which the information was created and by who, and
- the terms of the contractual arrangements between the agency and the service provider – for example whether the contract includes provisions concerning:
  - who can access or use information and for what purposes

- the circumstances in which information can be disclosed and to whom it may be disclosed
- the duration of the access and use of the information by the service provider
- consequences for misuse of personal information
- the disposal or the return of personal information on completion of the contract term
- indemnification of costs in the event of claims against the agency due to the action of the service provider.

Agencies should be aware that in order for the information to be considered to be "held", it is not a requirement that all of the factors are present.

Common types of contractual arrangements

Agencies have a range of contractual arrangements with service providers for the provision of services to government and for the provisions of services to the public on behalf of government.

Agencies should assess their current contractual arrangements and consider the factors outlined above to determine whether the service provider or the agency itself is the holder of personal information.

The following examples are not exhaustive and are provided as an illustration only. Agencies are strongly encouraged to seek their own legal advice on their specific contractual arrangements.

IT platforms, cloud storage and software-as-a-service

Almost all agencies will likely have contracts for IT services where agency information is hosted on IT infrastructure owned and operated by the service provider. This may include:

- email systems
- case management systems
- information management systems
- digital archives and cloud storage
- cloud-based IT services also known as Software-as-a-Service or Infrastructure-as-a-Service.

Under these arrangements, generally the agency will have the sole right to manage the information held within the system. In most cases the agency will be considered to hold any personal information within these systems due to the level of control exercised by the agency over this information.

Service provision to the public

Many agencies contract with private sector and not-for-profit organisations to provide services to the public.

Whether the agency will be considered to hold the personal information collected or used by the service provider will be a question of fact based on the specific arrangements in place and the terms of the contract governing these arrangements.

Agencies should carefully consider the arrangements in place for the provision of services to determine which entity holds the personal information.

Chain of contracts

Some service provision arrangements can involve a chain of multiple contracts. For example, an agency may enter into a contract with a service provider:

- who will then sub-contract one or more parts of its service provision to another organisation, or
- who will contract with another organisation for the provision of IT services.

Whether notification obligation arise for agencies in these circumstances, will require a detailed understanding of the terms of each contract in the chain, the nature of the information subject to the contractual arrangements and where that information is held. These arrangements can involve complex information governance arrangements and careful analysis will be required to determine which entity holds the personal information in the event of a data breach.

Contract terms

It is for each agency to determine the appropriate clauses to be incorporated into their procurement arrangements. Agencies are encouraged to review their standard procurement templates to ensure agencies are able to meet their notification obligations.

At a minimum, agencies should consider incorporating the following requirements into their procurement contracts:

- A requirement that the service provider promptly report data breaches to the agency, take mitigating actions and assist the agency in undertaking assessments.
- A statement of who should notify affected individuals and provide support in the event of the breach. As the organisation with the most direct relationship with the affected individuals the public sector agency will generally be best placed to notify and provide direct support as required.

Commonwealth Notifiable Data Breach Scheme

Most private sector entities will be subject to the Commonwealth Privacy Act 1998 and the Notifiable Data Breach Scheme (NDB Scheme) under that Act.

However, agencies should be mindful that the exemption under section 7B(5) of the *Privacy Act* will apply in relation to an act done or practice engaged in by a contracted service provider for a State contract. The effect of this is that the Information Protection Principles and the NDB Scheme may not apply to the private sector entity in the course of undertaking its contract with a NSW agency.

The service provider will only be subject to NSW privacy law if specifically required under the contract.

Other useful resources

Other resources that may be useful on this topic include:

- Guide to managing data breaches in accordance with the *Privacy and Personal Information Protection Act 1998*

For more information

Contact the Information and Privacy Commission NSW (IPC):

Freecall: 1800 472 679
Email: ipcinfo@ipc.nsw.gov.au
Website: www.ipc.nsw.gov.au

NOTE: The information in this fact sheet is to be used as a guide only. Legal advice should be sought in relation to individual circumstances.