NSW Public Sector Agencies and Notifiable Data Breaches

Fact sheet
February 2018

The Notifiable Data Breaches (NDB) scheme, under the federal *Privacy Act 1988* (Privacy Act), comes into effect on 22 February 2018.

The NDB scheme establishes a mandatory data breach notification scheme that requires organisations covered by the federal Privacy Act to notify individuals likely to be at risk of serious harm due to a data breach.

Although the NDB scheme is aimed primarily at federal government agencies and private sector organisations regulated by the Australian Privacy Principles (APPs) under the Privacy Act, there are provisions that apply to NSW public sector agencies.

Tax file number collection

Any agency that collects tax file numbers (TFNs) has obligations under the NDB scheme when a data breach occurs involving a TFN. This includes state and local government agencies, and public universities in NSW that routinely collect and hold TFN information.

A TFN is a unique number issued by the Australian Taxation Office (ATO) to identify individuals. TFN information is information that connects a TFN with the identity of a particular individual.

The *Privacy (Tax File Number) Rule 2015* (TFN Rule)[1] issued under s.17 of the Privacy Act, regulates the collection, storage, use, disclosure, security and disposal of individuals' TFN information. The TFN Rule requires any organisation holding TFNs to protect the information by implementing reasonable security safeguards in the circumstances.

The obligations under the TFN Rule are in addition to responsibilities under other laws, such as the *Privacy and Personal Information Protection Act 1998* (PPIP Act).

What is a TFN data breach?

A TFN data breach occurs where TFN information is lost, or subject to an unauthorised access or disclosure.

There are a number of ways this can occur. For example, if a database containing TFN information is hacked, if a TFN is mistakenly provided to the wrong person, or when paper records containing any TFN information are stolen.

When is a TFN data breach 'notifiable'?

The notification requirements under the NDB scheme will be triggered if the TFN data breach is 'likely to result in serious harm' to any individual.

Responding to a TFN data breach

Each TFN data breach will have to be dealt with on a case-by-case basis. However, there are four key steps to consider when responding to a breach:

1. Contain the breach

Depending on the type of TFN data breach, containing the breach may involve a range of responses. This could include searching for and recovering the TFN data, confirming that no copies were made or that the information was destroyed by the party receiving it, conducting a remote wipe on a lost portable device, implementing a computer system shut down, or changing passwords and system user names.

When a TFN data breach occurs you should conduct preliminary fact-finding about the breach (including cause, risk of spread, options to mitigate risk) and assess the risk posed by the breach.

It is important to inform the relevant key people in your organisation of the breach, such as the Privacy Officer and the Chief Executive Officer. In certain circumstances, it may also be necessary to inform the police.

2. Evaluate and mitigate the risks

Taking prompt remedial action will minimise the likelihood that the breach will result in harm to any individual. For example, depending on the type of data breach, employees might be told to change passwords, not to open emails with attachments, and to be aware of phishing attacks.

An assessment of the likely harm resulting from a TFN breach should be conducted as soon as practicable after an agency becomes aware of the breach. Ideally this will occur within 2-3 days but all reasonable steps must be taken to ensure the assessment is completed within 30 days.

The assessment should determine whether your agency reasonably believes that the loss, access or disclosure is 'likely to result in serious harm to any of the individuals to whom the information relates'. 'Serious harm' is not defined in the Privacy Act, but guidance from the Australian Privacy Commissioner suggests that it could

[1] https://www.legislation.gov.au/Details/F2015L00249

include such things as serious financial, physical, psychological, emotional or reputational harm.

3. Notification and communication

When the assessment at step 2 has been completed, notification (if required) must be commenced as soon as practicable.

Notification is required by law if the assessment has concluded that there are reasonable grounds to believe that the breach has resulted in, or is likely to result in, serious harm to one or more of the individuals to whom the information relates.

The notification requirements relate to notifying both the Australian Privacy Commissioner and the affected individuals.

A statement must be prepared about the TFN data breach which sets out the following:

- Identity and contact details of the agency that experienced the breach
- A description of the breach
- The kind or kinds of information concerned
- Recommendations about any steps that the individuals should take in response to the breach.

The statement may also include:

- any action that has been, or is being taken, to rectify the breach and mitigate any harm;
- details about any other party that has been notified (e.g. the NSW IPC or NSW Police); and
- if relevant, the identity and contact details of any other related organisations that are likewise affected by the data breach.

The statement must be sent to the Australian Privacy Commissioner at the Office of the Australian Information Commissioner (OAIC) as soon as practicable.

The statement must also be provided to the affected individuals as soon as practicable. As a minimum requirement, the statement must be*:*

1. provided directly to only those individuals at risk of serious harm; or
2. provided to all individuals whose TFN information was breached; or
3. (only if the affected individuals cannot be contacted directly) publicised more broadly.

This notification can be in the form of an email, letter or by phone contact. Additional steps may include a dedicated website, a media release or posts on social media.

Note: If NSW Police or another law enforcement agency is investigating the breach, they must be consulted before making details of the breach public.

4. Prevention of future breaches

Following a TFN data breach, agencies should fully investigate the cause of the breach and consider developing a prevention plan.

To mitigate the risk of any future data breaches, agencies may take a range of steps, including:

- a security audit and any modifications to physical controls such as locks, alarms, visitor access control;
- a review of policies and procedures including the privacy management framework;
- a review of employee training;
- a review of suppliers and third parties; and
- updating passwords, or altering deployments of technology.

More information about TFN data breaches

The OAIC has a dedicated website for the NDB scheme – see https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme.

In addition, further information about the handling of TFN information is available at: https://www.oaic.gov.au/privacy-law/privacy-act/tax-file-numbers.

To contact the OAIC, call 1300 363 992 or email enquiries@oaic.gov.au.

Other data breach notification schemes

In addition to the NDB scheme, there are two other data breach notification schemes which create responsibilities for NSW public sector agencies in certain circumstances.

A. Sharing of government sector data

The *Data Sharing (Government Sector) Act 2015* (DSGS Act) has a data breach notification scheme in respect of sharing of government sector data under the DSGS Act with the NSW Data Analytics Centre, or between other government sector agencies.

If an agency that is receiving personal or health information under the DSGS Act becomes aware that privacy legislation has been (or is likely to have been) breached, the agency must, as soon as practicable, inform the data provider and the NSW Privacy Commissioner (IPC) of the breach.

B. European Union's General Data Protection Regulation

The *General Data Protection Regulation* (GDPR) will apply from 25 May 2018 to any organisation offering goods or services to, or monitoring the behaviour of, individuals living in the European Union (EU). This may include some NSW public sector agencies (e.g. universities offering educational packages to international students).

The data breach notification requirements under the GDPR include notification to the relevant EU supervisory authority within 72 hours after having become aware of the breach.

Further information is available from the OAIC.

Notification of data breaches to the IPC

As a matter of best practice, agencies are encouraged to voluntarily report all other types of data breaches to the IPC, and to affected individuals as appropriate. This may include data breaches involving personal information other than TFNs, or data breaches involving TFNs but which are *not* likely to result in serious harm.

Notification should contain similar content to that provided to individuals/organisations. The personal information about the affected individuals is not required. It may be appropriate to include:

- a description of the breach;
- the type of personal information involved in the breach;
- what response the agency has made to the breach;
- what assistance has been offered to affected individuals;
- the name and contact details of the appropriate contact person; and
- whether the breach has been notified to other external contact(s).

Having a data breach procedure or policy can make it easier to handle a data breach. The IPC has proactively released its *IPC Data Breach Policy* and agencies are encouraged to refer to it when reviewing their own policies. The *IPC Data Breach Policy* is available on the IPC website.

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