National Education and Care Services Privacy Commissioner

NECS Privacy Information Sheet 1

February 2018

Notifiable Data Breaches Scheme - Advice to Regulatory Authorities and ACECQA

Section 263 of the Education and Care Services National Law applies the Commonwealth Privacy Act 1988, as in force from time to time, as a law of a participating jurisdiction for the purposes of the National Quality Framework. Regulation 199 of the Education and Care Services National Regulations modifies the Privacy Act to apply specifically to agencies, those agencies being the National Authority (ACECQA) and each State and Territory Regulatory Authority of a participating jurisdiction. Regulation 196 of the Education and Care Services National Regulations modifies the Privacy Act 1988 to mean that a reference to the Australian Information Commissioner is a reference to the National Education and Care Services Privacy Commissioner.

The Privacy Amendment (Notifiable Data Breaches) Act 2017 establishes the Notifiable Data Breaches (NDB) Scheme under Part IIIC of the Privacy Act. The NDB scheme applies from 22 February 2018 to all agencies and organisations with existing personal information security obligations under the Privacy Act. These include ACECQA and each of the State and Territory Regulatory Authorities (referred to as the agencies throughout this Information Sheet).

Relevant sections of the Privacy Act are referred to throughout this Information Sheet.

What is the NDB Scheme?

The Notifiable Data Breaches (NDB) scheme establishes requirements for entities in responding to data breaches. Entities have data breach notification obligations when a data breach is likely to result in serious harm to any individual whose personal information is involved in the breach.

The NDB scheme places an obligation on ACECQA and State and Territory Regulatory Authorities to notify individuals whose personal information is involved in a data breach that is likely to result in serious harm. The NECS Privacy Commissioner must also be notified.

What data breaches require notification?

The NDB scheme only applies to data breaches involving personal information that are likely to result in serious harm to any of the individuals to whom the information relates. These are referred to as 'eligible data breaches'.

An eligible data breach arises when the following three criteria are satisfied:

- there is **unauthorised access** to or **unauthorised disclosure** of personal information, or a **loss** of personal information, that an agency holds, and

- a reasonable person would conclude that this is likely to result in **serious harm** to one or more individuals to whom the information relates, and

- the agency has not been able to prevent the likely risk of serious harm with **remedial action**.

Assessing for unauthorised access, disclosure or loss.

Agencies must be prepared to conduct a quick assessment of a suspected data breach to determine whether it is likely to result in serious harm to any individual and as a result require notification. S26WH(2)(b) of the Privacy Act requires agencies to take all reasonable steps to ensure the assessment is completed within 30 days of the agency becoming aware there may have been an eligible data breach.

Unauthorised access of personal information occurs when personal information that an agency holds is accessed by someone who is not permitted to have access. This includes unauthorised access by an employee of the entity, or an independent contractor, as well as unauthorised access by an external third party (such as by hacking).

Unauthorised disclosure occurs when an agency, whether intentionally or unintentionally, makes personal information accessible or visible to others outside the agency, and releases that information from its effective control in a way that is not permitted by the Privacy Act. This includes an unauthorised disclosure by an employee of the agency.

Loss refers to the accidental or inadvertent loss of personal information held by an entity, in circumstances where is it is likely to result in unauthorised access or disclosure.

Assessing for the nature and likelihood of "serious harm"

The second step in deciding whether an eligible data breach has occurred involves deciding whether, from the perspective of a **reasonable person**, the data breach would be **likely to result** in **serious harm** to an individual whose personal information was part of the data breach.

"Reasonable person" is not defined in the Privacy Act. For the purposes of the NDB scheme it is taken means a person in the agency's position (rather than the position of an individual whose personal information was part of the data breach or any other person), who is properly informed, based on information immediately available, or following reasonable inquiries or an assessment of the data breach.

The phrase 'likely to result' means the risk of serious harm to an individual is more probable than not (rather than possible).

"Serious harm" is also not defined in the Privacy Act. In the context of a data breach, serious harm to an individual may include serious physical, psychological, emotional, financial, or reputational harm. Examples may include:
- identity theft
- significant financial loss by the individual
- threats to an individual's physical safety
- loss of business or employment opportunities
- humiliation, damage to reputation or relationships
- workplace or social bullying or marginalisation.

The NDB scheme includes a non-exhaustive list of 'relevant matters' that may assist agencies to assess the likelihood of serious harm. These are set out in s26WG of the Privacy Act as follows (paraphrased):
- the kind of information;
- the sensitivity of the information;
- whether the information is protected by any security measures;
- if the information is protected by security measures and the likelihood that any of those security measures could be overcome;
- the persons, or the kinds of persons, who have obtained, or who could obtain, the information;
- if a security measure (eg encryption) was used in relation to the information, and was designed to make the information unintelligible or meaningless to persons unauthorised to obtain the information, the likelihood that anyone obtaining the information with the intention of causing harm would have access to information or knowledge required to circumvent the security measures;
- the nature of the harm;
- any other relevant matters.

Remedial Action

The NDB scheme provides agencies with the opportunity to take positive steps to address a data breach in a timely manner and avoid the need to notify. If an agency takes remedial action such that the data breach would not be likely to result in serious

harm, then the breach is not an eligible data breach for that agency or for any other agency. For breaches where information is lost, the remedial action is adequate if it prevents unauthorised access to, or disclosure of personal information.

If the remedial action prevents the likelihood of serious harm to some individuals within a larger group of individuals whose information was compromised in a data breach, notification to those individuals for whom harm has been prevented is not required.

Requirement to Prepare and Provide a Statement about an Eligible Data Breach

If, following assessment, an agency has reasonable grounds to believe that there has been an eligible data breach the agency **must prepare a statement and provide a copy to the NECS Privacy Commissioner.** S26WK(3) of the Privacy Act requires the Statement to include:

(a) the identity and contact details of the agency;

(b) a description of the eligible data breach that the agency believes has happened;

(c) the kind or kinds of information concerned; and

(d) recommendations about the steps that individuals should take in response to the breach.

If the agency has reasonable grounds to believe that the eligible data breach also constitutes an eligible data breach of one or more other agencies the statement may also set out the identity and contact details of those agencies.

Requirement to Notify Individuals

S26WL of the Privacy Act requires an agency that has prepared a Statement about an eligible data breach to:

(a) take reasonable steps to notify the contents of the Statement to each of the individuals to whom the relevant information relates; or

(b) take reasonable steps to notify the content of the Statement to each of the individuals who are at risk from the eligible data breach, or

(c) if it is not practicable for (a) or (b) to occur, publish a copy of the Statement on the agency's website and take reasonable steps to publicise the contents of the Statement.

Agencies can also provide further information in their notification such as an apology and an explanation about what they are doing about the breach.

Action to prevent Future Breaches

Following a data breach, agencies should review the incident and take action to prevent future breaches. This may include:
- fully investigating the cause of the breach;
- developing a prevention plan;
- conducting regular audits to ensure the plan is implemented and maintained;
- updating security;
- changes to policies and procedures;
- staff training.

Role of the NECS Privacy Commissioner under the NDB Scheme

The NECS Privacy Commissioner has a number of roles under the NDB scheme. These include:

- receiving notifications from ACECQA and State and Territory Regulatory Authorities of eligible data breaches;

- making enquiries or offering advice and guidance in response to notifications;

- encouraging compliance with the scheme, including by handling complaints, conducting investigations, and taking other regulatory action in response to instances of non-compliance;

- offering advice and guidance to ACECQA and Regulatory Authorities and providing information to the community about the operation of the scheme.

The NECS Privacy Commissioner has a range of enforcement powers to ensure that agencies meet their obligations under the scheme. A failure by an agency to meet any of the following requirements of the scheme is an interference with the privacy of an individual under s13(4A) of the Privacy Act:
- conduct a reasonable and expeditious assessment of a suspected eligible data breach (s 26WH(2)), taking all reasonable steps to ensure that this assessment is completed within 30 days of becoming aware (s 26WH(2)(b))

- prepare a statement about the data breach, and give a copy to the Commissioner, as soon as practicable (s 26WK(2))
- notify the contents of the statement to individuals at risk of serious harm (or, in certain circumstances, publish the statement) as soon as practicable (s 26WL(3))
- comply with a direction from the Commissioner to prepare a statement and notify as soon as practicable (s 26WR(10)).

The preferred approach of the NECS Privacy Commissioner is always to work with agencies to encourage and facilitate voluntary compliance with the agencies' obligations under the Privacy Act before taking any enforcement action.

Should they become necessary, enforcement powers available to the NECS Privacy Commissioner in response to an interference with privacy include powers to:
- accept an enforceable undertaking (s 33E) and bring proceedings to enforce an enforceable undertaking (s33F)
- make a determination (s52) and bring proceedings to enforce a determination (ss55A and 62)
- seek an injunction to prevent ongoing activity or a recurrence (s98)
- apply to court for a civil penalty order for a breach of a civil penalty provision (s80W), which includes a serious or repeated interference with privacy (s13G).

The NECS Privacy Commissioner can also direct an agency to notify individuals at risk of serious harm, as well as the Commissioner, about an eligible data breach in certain circumstances (s26WR). This might happen if a data breach comes to the attention of the Commissioner but has not come to the attention of the agency, or if the Commissioner does not agree with the agency's initial view about whether a data breach triggers an obligation to notify.

If the Commissioner and the agency cannot agree about whether notification should occur, the Commissioner will give the agency an opportunity to make a formal submission about why notification is not required, or if notification is required, on what terms. The Commissioner will consider the submission and any other relevant information before deciding whether to direct the entity to notify under s26WR.

Before directing an agency to notify, the Commissioner will usually ask the agency to agree to notify.

The NECS Privacy Commissioner may also declare that notification of a particular data breach is not required (s26WQ(1)(c)) if satisfied it is reasonable in the circumstances to do so, and the Commissioner may also modify the period in which notification needs to occur (s26WQ(1)(d)).

Resources

The *Privacy Amendment (Notifiable Data Breaches) Act 2017* is available at: www.legislation.gov.au/Details/C2017A00012

The Australian Information Commissioner website at www.oaic.gov.au contains further explanatory information and resources about the NDB Scheme which will be used, and adapted where necessary, by the NECS Privacy Commissioner in oversighting the application of the NDB Scheme by ACECQA and the State and Territory Regulatory Authorities.

Acknowledgement

The information provided in this Information Sheet is drawn from the *Privacy Amendment (Notifiable Data Breaches) Act 2017* and material developed by the Commonwealth Office of the Australian Information Commissioner, modified to reflect the specific jurisdiction and circumstances of the NECS Privacy Commissioner.

The information is of a general nature. It is not a substitute for legal advice.