A summary of the Notifiable Data Breach reporting scheme

From 22 February 2018 new privacy laws commence to mandate the reporting of eligible privacy and data breaches to the OAIC and impacted individuals with limited exceptions. This is generally known as the notifiable data breach reporting scheme (NDB).

The new S26 of the Privacy Act 1988 (Cth) specifies these obligations and brings Australia in line with jurisdictions such as most of the EU, UK, Japan and most US states that already have mandatory reporting regimes.

From May 2018 organisations operating in the EU will also be impacted by the new General Data Protection Regulations (GDPR) which imposes substantial obligations and penalties on organisations acting through jurisdictions throughout Europe including penalties of up to 4% of global annual turnover for breaches with a cap of 20,000 euros.

TAL has been following the progress of the new privacy legislation including membership and chair of the FSC Working Group on Privacy FSC submissions and involvement in co-authoring submissions on the legislation.

TAL is taking proactive steps to prepare for the commencement of the NDB scheme including, but not limited to, the following items:

- Reviewing current processes, policies and procedures regarding the identification, management, notification and rectification of data breaches;
- Reviewing current privacy and information security processes and documented procedures to meet current information security obligations including data transmission processes;
- Reviewing current privacy, security and cyber-security provisions in contracts with key stakeholders including outsourced service providers, business partners;
- Reviewing and updating our Data Breach Response Plan to incorporate the requirements of the new NDB scheme including the assessment of an 'eligible data breach" for "likely risk of serious harm" and a process to decide whether or not notification to the impacted individuals and/or the OAIC is required;
- Reviewing and updating where relevant, existing customer materials referring to privacy and security controls;
- Keeping updated on publications from the OAIC regarding the NDB scheme and attending relevant industry conferences to obtain intelligence and keep up to date with how the financial services industry is responding to the new obligations; and
- Rolling out specific training staff on the new obligations.

A brief summary of the NDB scheme and a link to OAIC resources is set out below and is subject to this disclaimer.

Disclaimer: The content including publications or links to external websites supplied to you by TAL Life Limited ABN 70 050 109 450 AFSL 237848 or its related bodies and subsidiaries, is intended only to provide a summary and general overview on matters regarding notifiable data breaches. Information shared is not intended to be comprehensive nor does it constitute legal advice, it is also as it applies directly to TAL Life Limited and its related bodies and subsidiaries and this information cannot directly be applied to any other companies or organisations outside of TAL. We attempt to ensure that the shared content is current but we do not guarantee its currency. You should seek legal or other professional advice before acting or relying on any of the content or information shared and supplied. TAL is not responsible to you or anyone else for any loss suffered in connection with the use of this shared content. The shared content may be subject to Copyright and other licensing laws.

Summary of the new obligations

Organisations are expected to have policies and procedures in place that outline the steps that must be taken in response to a privacy breach including a Data Breach Response Plan and policies setting out expectations of staff when collecting, using, securing and disclosing customer information.

When an organisation identifies an eligible data breach it must assess the breach to ascertain if notification to the OAIC and impacted individuals is required. Organisations are required to complete this assessment within 30 days but are also expected to complete a "reasonable and expeditious" assessment of the breach.

Eligible breaches and criteria for likely risk of serious harm: A privacy/data breach will arise:

- where there has been unauthorised access to, or unauthorised disclosure of, personal information about one or more individuals; or
- where information has been lost and could be accessed or disclosed by unauthorised people or entities.

An eligible data breach arises where a reasonable person would conclude that there is "a likely risk of serious harm" to any of the impacted individuals as a result of the unauthorised access or disclosure.

Serious harm includes physical harm, financial/economic harm, emotional harm (e.g. embarrassment and humiliation), psychological harm (e.g. marginalisation and bullying) and reputation harm.

Whether or not there is a likely risk of serious harm will depend on the circumstances of the impacted individual which may or may not be known to the organisation. Serious harm will be likely if such harm is more probable than not having regard to:

- the security measures put in place by the organisation (e.g. if the data is encrypted/password protected, anonymous, tokenised etc.);
- the extent and sensitivity of the information;
- the potential for exploitation or misuse of the information (e.g. credit card details, bank details, TFN's etc.)

Serious harm will be likely if such harm is more probable than not having regard to all relevant matters.

Organisations are expected to prepare a statement to give notice of an eligible data breach when notifying the OAIC. The statement should be sent as soon as is practicable after identifying the breach and must include:

- the identity and contact details of the entity;
- a description of the serious data breach that the Commissioner has reasonable grounds to believe has happened;
- the kinds of information concerned; and
- recommendations about the steps that individuals should take in response to the data breach that the Commissioner has reasonable grounds to believe has happened.

An organisation must:

- if it is practicable to do so, take such steps as are reasonable in the circumstances to notify each of the individuals to whom the relevant information compromised in an eligible data breach relates; or
- if it is practicable to do so, take such steps as are reasonable in the circumstances to notify those individuals who are considered to be 'at risk' from the eligible data breach; or
- if it is not practicable to notify via either of the above two methods, make a statement by publishing the statement on the entity's website and taking reasonable steps to publicise the statement.
- Organisations are expected to provide impacted individuals with general advice about steps they should take to mitigate the harm that may arise to them as a result e.g. checking transactions on their policies or bank/credit card accounts.

Exceptions: Remedial action exception: If an organisation takes remedial action before any serious harm is caused by the breach the notification does not need to be made. This covers the situation where an eligible data breach occurs but the entity which experienced the eligible data breach is able to take action so that a reasonable person would conclude that an unauthorised access, unauthorised disclosure, or loss, as the case may be, would not be likely to result in serious harm to any of the individuals to whom the information relates.

A similar exception applies where an entity takes action that prevents unauthorised access or unauthorised disclosure from occurring following a loss of information. If the action remediates harm only to a particular individual or individuals from a larger cohort of individuals whose information was compromised in an eligible data breach, notification to those particular individuals is not required.

If, as a result of the action, a reasonable person would conclude that the access or disclosure would not be likely to result in serious harm to any of the individuals to whom the information relates, the eligible data breach is not, and is taken never to have been, an eligible data breach of the entity concerned.

NDB scheme resources: The OAIC has published draft resources on the mandatory data/privacy breach notification scheme which will be finalised over the coming months with input from industry.

https://www.oaic.gov.au/engage-with-us/consultations/notifiable-data-breaches/

These resources include the following:

- What is the Notifiable Data Breaches scheme?
- What is a Notifiable Data Breach?
- Why is the Notifiable Data Breach scheme important?
- When does the Notifiable Data Breach take effect?
- Resources for organisations to prepare for the Notifiable Data Breach scheme.
- Organisations that must comply with the Notifiable Data Breach scheme.
- Which data breaches are notifiable?
- Resources for assessing suspected data breaches.
- How to notify the OAIC and impacted individuals?
- The role of the OAIC in the Notifiable Data Breach scheme regulation.
- How to keep informed about developments regarding the Notifiable Data Breach scheme?

Other related OAIC resources: The OAIC has published its expectations regarding what steps organisations are expected to have in place to protect personal information and prevent data breaches:

https://www.oaic.gov.au/agencies-and-organisations/app-guidelines/chapter-11-app-11-security-of-personal-information

https://www.oaic.gov.au/agencies-and-organisations/guides/guide-to-securing-personal-information

The OAIC has also published its expectations regarding data breach response plans and conducting a privacy impact assessment.
https://www.oaic.gov.au/agencies-and-organisations/guides/guide-to-developing-a-data-breach-response-plan

https://www.oaic.gov.au/agencies-and-organisations/guides/guide-to-undertaking-privacy-impact-assessments