BRIEFING PAPER

Privacy Update:
Mandatory Notification of Data Breaches

The information in this briefing paper is current as at May 2017

CompliSpace Pty Ltd 1300 132 090
www.complispace.com.au
ACT | NSW | NT | QLD | SA | TAS | VIC | WA

Published by:

complispace
make it work

TABLE OF CONTENTS

1. Executive Summary

Commencing on 22 February 2018, changes to the federal Privacy Act make it compulsory for organisations to notify specific types of data breaches (Notifiable Data Breaches or NDBs), to individuals affected by the breach, and to the Office of the Australian Information Commissioner (OAIC). A data breach occurs where "personal information held by an agency or organisation is lost or subjected to unauthorised access, modification, disclosure, or other misuse or interference."

As with most of the Privacy Act, this requirement applies to all private organisations, unless they have a revenue of less than $3 million.

Not all data breaches will be NDBs. A NDB is defined as a data breach that is likely to result in **serious harm** to any of the individuals to whom the information relates. Serious harm could include serious physical, psychological, emotional, economic and financial harm, as well as serious harm to reputation.

To comply with the NDB requirements organisations will need to have procedures in place which are known and understood by employees, and integrated into their existing documented Privacy Program, to ensure that data breaches are identified and dealt with as required by the Privacy Act's NDB scheme. A key element of this is that organisations should develop a **data breach response plan** so that employees understand their roles and responsibilities should a notifiable breach occur.

The NDB changes to the Privacy Act highlight the need for organisations to have implemented their Privacy Programs as required by the 2014 changes to the Privacy Act. This means that if an organisation has not yet taken steps to ensure that the personal information it collects is managed in accordance with the Act, they will be exposed to serious reputational damage if a NDB occurs, as well as the risk of serious financial penalties if the breach was due to failure to comply with the Privacy Act's 13 Australian Privacy Principles (APPs).

If you are one of the many organisations who may not have a Privacy Program in place, or even a Privacy Policy for that matter, you are running the risk of a significant data breach occurring – potentially jeopardising not only the security of your clients' personal information, but also having serious consequences for your organisation.

To comply with these changes, organisations should start by conducting a **Personal Information Management Audit** to test the security of their personal information protection processes and procedures.

2. Background: Purpose of the Notifiable Data Breach Scheme

The 2014 amendments to the Privacy Act introduced 13 Australian Privacy Principles (APPs) which apply to private sector organisations. Failure to comply with the APPs can result in significant penalties.

The NDB amendment to the Act was introduced to give effect to an earlier report of the Australian Law Reform Commission which found that as more and more information was being held in electronic format the risk of breaches in security protecting that data was also greatly increased.

The amendment closes one of the gaps in the legislation, with the requirement for an organisation to report breaches rather than waiting for an injured party to notice that their data was being misused and then complaining about it.

The key to protecting data so that a breach does not arise is APP 11, which requires an organisation to take 'reasonable steps' to protect the personal information it holds from misuse, interference and loss, as well as unauthorised access, modification or disclosure.

It is clear that an organisation's failure to comply with APP 11 could lead to personal data being subject to unauthorised access, disclosure or use. Until now, organisations were encouraged to voluntarily report the breach to the OAIC themselves, but even if an organisation did decide to disclose, there was no requirement that the affected individuals were to be informed nor was there a requirement that this occur within a reasonable time frame.

3. What is a Notifiable Data Breach?

Not all instances of unauthorised access to or use of personal information will come under the mandatory reporting regime. The Privacy Act refers to an "eligible data breach", while the OAIC uses the term NDB on its website.

Under the Act a data breach must be notified where:

- ✓ there is unauthorised access to, or unauthorised disclosure of, personal information; and
- ✓ a reasonable person would conclude that the access or disclosure would be likely to result in **serious harm** to any of the individuals to whom the personal information relates.

OR

Personal information is lost in circumstances where:

- ✓ unauthorised access to, or unauthorised disclosure of, the information is likely to occur; and
- ✓ assuming that unauthorised access to, or unauthorised disclosure of, the information were to occur, a reasonable person would conclude that the access or disclosure would be likely to result in **serious harm** to any of the individuals to whom the information relates.

Examples of a data breach which may meet the definition of an eligible data breach include when:

- ✓ a device containing an employee's personal information is lost or stolen eg a laptop;
- ✓ a database containing personal information is hacked; or
- ✓ personal information is mistakenly provided to the wrong person.

Serious Harm

The Explanatory Memorandum to the Act explains that **serious harm** could include serious physical, psychological, emotional, economic and financial harm, as well as serious harm to reputation and other forms of serious harm that a reasonable person in the organisation's position would identify as a possible outcome of the data breach.

The Explanatory Memorandum also emphasises that though individuals may be distressed or otherwise upset at an unauthorised access to or unauthorised disclosure or loss of their personal information, this would not in itself be sufficient to require notification unless a reasonable person in the organisation's position would consider that the likely consequences for those individuals would constitute serious harm. It is expected that a likely risk of serious financial, economic or physical harm would be the most common likely forms of "serious harm" that may give rise to the notification.

4. What Needs to Happen When There Has Been a Notifiable Data Breach?

Where an eligible data breach is suspected or believed to have occurred an organisation must:

- ✓ Carry out a risk assessment in the event that an eligible data breach is suspected;
- ✓ Prepare a statement of prescribed information regarding an eligible data breach that is believed to have occurred;
- ✓ Submit the statement to the OAIC; and
- ✓ Contact all affected individuals directly or indirectly by publishing information about the eligible data breach on publicly accessible forums.

Each of these steps is explained in more detail below.

Suspected Eligible Data Breach

If an organisation suspects an eligible data breach may have occurred it must conduct a risk assessment which involves:

- ✓ assessing whether there are reasonable grounds to believe that the relevant circumstances amount to an eligible data breach. This must be as prompt and efficient as practicable in the circumstances; and
- ✓ taking all reasonable steps to ensure that the assessment is completed within 30 days after becoming aware of the breach.

An organisation may be required to undertake a risk assessment where an individual has made a complaint in relation to the security of personal information and the organisation suspects that an eligible data breach may have occurred, but further information is required to ensure the criteria of an "eligible data breach" is met.

If the risk assessment reveals that an eligible data breach has occurred, the organisation must then follow the notification requirements under the Act and notify both the OAIC and if practicable, the individual/s affected.

Notifying the OAIC

Once an organisation has reasonable grounds to believe that there has been an eligible data breach, the organisation must:

- ✓ prepare a Statement in the prescribed format; and
- ✓ give a copy of the statement to the OAIC as soon as practicable after the organisation becomes aware of the eligible data breach.

The Statement must set out:

- ✓ the identity and contact details of the organisation;
- ✓ a description of the eligible data breach that the organisation has reasonable grounds to believe has happened;
- ✓ the kind/s of information concerned; and
- ✓ recommendations about the steps that individuals should take in response to the eligible data breach that the organisation has reasonable grounds to believe has happened.

If the organisation believes that another entity regulated by the Act is involved in the eligible data breach, the Statement must include information about the other entity/ies.

Notifying the Individual/s

As soon as practicable after notifying the OAIC, the organisation must, if it is **practicable**:

- ✓ notify each of the individuals to whom the relevant information relates; or
- ✓ notify each of the individuals who are *at risk* from the eligible data breach.

In each case, the organisation must take "such steps as are reasonable in the circumstances" to notify the individuals. What is **practicable** will involve considerations about the time, effort or cost of a notification.

If neither of the above options apply, the organisation must:

- ✓ publish a statement on its website; and
- ✓ take reasonable steps to publicise the contents of the Statement it prepared for the OAIC.

If the publication option is taken, the organisation should choose the publication channels most likely in the circumstances to be effective in bringing the eligible data breach to the attention of affected individuals.

OAIC's Power to Direct the Organisation

If the organisation has not already done so, the OAIC may direct it to provide a notification to it and notify affected individuals, if the OAIC is aware that reasonable grounds exist to believe that there has been an eligible data breach at the organisation.

AFSL Obligations

If an organisation that is an AFS licence holder identifies a data breach that amounts to a breach of APP 11, it will also need to consider if the breach amounts to a contravention of its obligations under the Corporations Act 2001 (Cth) (Corporations Act).

The organisation will need to determine if the breach is a significant breach and/or if it is also a responsible entity, whether the breach is a material breach. The significance of an eligible data breach needs to be considered in light of the factors included in sections 912A and 912D of the Corporations Act. The reporting requirements for a responsible entity under section 601FC must also be considered.

If you determine that the breach is significant and/or material, a breach report must be submitted to ASIC in addition to reporting the matter to the OAIC.

5. Compliance with the NDB Scheme

To comply with the 2014 amendments to the Act, organisations needed to implement internal practices, procedures and systems, integrated within their operational framework, to ensure that they comply with each of the 13 APPs and are able to deal with enquiries or complaints from individuals about their compliance.

A key message we have sought to deliver since 2014 has been that "simply publishing a privacy statement on your public website is not enough." This is because practicing privacy everyday involves more than just directing employees and other individuals to your privacy policy. Employees need to understand how all of

their daily activities, including sending emails, and answering phones, can include personal information of some sort which must be handled in accordance with the law.

Given the broad range of personal information (including sensitive information) of thousands of individuals (employees, clients, prospective clients, job applicants, ex-employees, volunteers/contractors), it is strongly recommended that an organisation undertake the work necessary to comply with the 13 APPs if they have not done so already.

6. Next Steps for Organisations

Policies and Procedures

With the passing of the Privacy Act amendment relating to Notifiable Data Breaches in February 2017, organisations are effectively on notice to ensure that they have developed and implemented a Privacy Program so that the employees of the organisation understand how to protect personal information in accordance with APP 11. If an organisation has implemented a compliant Privacy Program, it should take the following steps in order to comply with the additional requirements of the NDB amendments:

- ✓ review and test the strength of its security measures which protect personal information and establish any compliance gaps (a **Personal Information Management Audit** can be used for this purpose);
- ✓ review the information in the OAIC's APP 11 Guidance Materials which may assist your organisation to manage any compliance gaps;
- ✓ develop procedures to ensure the organisation's NDB obligations will be met if an eligible data breach occurs;
- ✓ communicate the NDB procedures to employees and other relevant individuals; and
- ✓ as part of its **risk management** procedures, train all employees with respect to their privacy obligations and the NDB requirements.

If an organisation has been tardy in complying with the APPs, it will be at a much higher risk of data breaches occurring. From a commercial perspective, a lack of compliance with the Privacy Act may demonstrate a weakness in an organisation's general approach to risk management. In order to comply with the NDB requirements, the organisation will have a higher workload ahead to catch up with implementing the policies and procedures necessary to comply with all of the obligations under the Privacy Act.

Data Breach Response Plan

The OAIC recommends that organisations develop a data breach response plan (DBR Plan) to enable them to contain, assess and respond to data breaches, including NDBs, to help mitigate potential harm to affected individuals. The OAIC has produced a Guide to developing a data breach response plan which sets out the roles and responsibilities for managing an appropriate response to a data breach as well as describing the steps to be taken by an entity in managing a breach if one occurs.

Developing a DBR Plan is not mandatory, however doing so is an example of taking 'reasonable measures' to protect personal information under APP 11. Organisations should consider developing a DBR Plan as part of their work to comply with their new obligations.

7. Additional Resources

The OAIC has released some initial high-level guidance for organisations to prepare for the beginning of the NDB requirements in February 2018, with the promise of more guidance information and events to come.

8. How CompliSpace Can Help

CompliSpace combines specialist governance, risk and compliance (GRC) consultancy services with practical, technology-enabled solutions. We are the leading provider of privacy law GRC services in Australia, working with leading AFSL holders and other private sector organisations in all Australian states and territories.

Our team of lawyers and industry experts actively monitor changes to relevant laws and standards and deliver a full suite of online policies, procedures and governance programs that enable organisations to continuously comply with their legal and regulatory obligations.

In response to the introduction of the NDB scheme, CompliSpace has developed detailed policies and procedures, including a DBR Plan that address the provisions under the legislation. The new policies and procedures are designed to integrate into an organisation's existing Privacy Program and be tailored to the particular circumstances of each organisation. CompliSpace has also developed detailed online privacy training which includes information on the NDB scheme.

CompliSpace works with organisation to tailor compliance and risk management systems to an organisation's individual needs and characteristics, ensuring meaningful compliance with their legal and regulatory obligations.

If you are looking to update your existing privacy content, contact us on:
T: 1300 132 090 **E:** contactus@complispace.com.au **W:** www.complispace.com.au
CompliSpace Media is the publisher of the CompliSpace Blog: www.complispace.com.au/blog

Disclaimer

This briefing paper is a guide to keep readers updated with the latest information. It is not intended as legal advice or as advice that should be relied on by readers. The information contained in this briefing paper may have been updated since its posting, or it may not apply in all circumstances. If you require specific advice, please contact us on 1300 132 090 and we will be happy to assist.