BRIEFING PAPER

Privacy Update:
Mandatory Notification of Data Breaches & the Opportunity to Increase Trust

The information in this briefing paper is current as at October 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

- ✓ In May 2017 we published a briefing paper: Privacy Update: Mandatory Notification of Data Breaches (May Paper). The May Paper explained one of the most important reforms since the introduction of the 13 Australian Privacy Principles (APPs) in 2014: the incoming federal Notifiable Data Breach Scheme (NDB Scheme).
- ✓ The NDB Scheme takes effect on **22 February 2018**.
- ✓ Failure to comply with the notification requirements under the NDB Scheme may result in penalties under the Privacy Act including fines of $420,000 for individuals and $2.1 million for organisations. In addition, a NDB may also be 'significant breach' of an AFSL holder's obligations under the Corporations Act reportable to ASIC.
- ✓ Australian regulators beyond the Office of the Australian Information Commissioner (OAIC), including ASIC, the ASX and APRA are increasing their focus on cyber security and privacy compliance, meaning that organisations should not ignore the importance of dedicating internal resources to these key areas of corporate governance.
- ✓ Organisations that simply have a privacy policy published on its website will find that this is insufficient to meet the NDB scheme. We recommend that organisations have a Privacy Program in place which addresses the 13 APPs and the NDB in addition to their privacy policy to ensure that they are able to meet their obligations.

While the May Paper focused on the legal aspects of the NDB Scheme, this paper discusses the key governance and strategic reasons why your organisation should care about compliance with the NDB Scheme. This paper explains:

- ✓ How organisations should use recently released OAIC guidance
- ✓ How regulators including ASIC, the ASX and APRA are addressing the issue of data security and in particular, how ASIC's Corporate Plan for 2017–18 to 2020–21 (Corporate Plan) will impact upon an organisation's approach to privacy and data security
- ✓ What the AICD is saying about cybersecurity and the NDB Scheme in its latest Essential Director Update: 17
- ✓ What practical steps organisations should be taking now to ensure compliance with the NDB Scheme by 22 February 2018
- ✓ The work CompliSpace has done to update the policies and procedures in our Privacy Program to ensure that the Program is up-to-date and available for implementation and use by organisations by 22 February 2018.

2. OAIC Guidance

Since the May Paper the OAIC has been busy publishing multiple new resources on the NDB Scheme on its website:

- ✓ Draft: Identifying eligible data breaches (June)
- ✓ Draft: Notifying individuals about an eligible data breach (June)
- ✓ Draft: Exceptions to notification obligations (September)
- ✓ Draft: Assessing a suspected data breach (September)
- ✓ Draft: What to include in an eligible data breach statement (September)
- ✓ Draft: Notifiable Data Breach statement (September).

The OAIC resources include useful information about the practical application of the NDB Scheme requirements. However, as they remain in draft format, organisations should not rely on the accuracy of their contents. It is unclear when those resources will become final.

3. Regulatory Landscape: Data Security

Regulatory convergence is becoming increasingly common in the Australian regulatory landscape. To understand how the NDB impacts your organisation beyond the Privacy Act and the OAIC we have summarised below how this requirement has been addressed by regulators across the Australian regulatory landscape being, ASIC, the ASX and APRA. The regulators' views are also supported by Australia's leading governance industry representative, the AICD.

ASIC

ASIC has identified that cyber threats, including threats to customers' personal information, are one of the main risks facing the financial sector.

On 1 September 2017 ASIC published its Corporate Plan which identified data security and privacy as one of its key challenges and areas of focus over the next 12 months. Specifically, ASIC is focused on how an organisation ensures the security of the data, including personal information that it manages. Some of those risks and challenge are listed below as well as the recommended compliance action to take to manage and respond to those risks and challenges.

ASIC Challenge / Risk	Compliance Action
Lack of customer trust and confidence in an organisation's data storage and sharing arrangements	Establishing an up to date Privacy Program which complies with the NDB Scheme is an obvious way of ensuring key stakeholders have confidence in the security of an organisation's data storage and sharing arrangements.
Corporate governance practices are unsound and do not support market integrity and good investor outcomes	Establishing an up to date Privacy Program which complies with the NDB Scheme is an example of a solid corporate governance practice. Having procedures in place to protect personal information and manage data breaches if they occur will minimise the risk of reputational damages, supporting good investor outcomes.
Digital disruption and cyber resilience in financial services and markets	It goes without saying that having an effective Privacy Program will not only help an organisation to manage the risk of digital disruption but will also enhance cyber resilience.

Organisations should be guided by ASIC's strategic focus to influence their own corporate strategy on privacy and data security. Doing so will not only ensure they achieve a risk and compliance culture but should also minimise their regulatory interaction with ASIC itself if the organisation is an AFSL holder. This is because if an AFSL holder identifies a data breach that is a contravention of the APPs, the breach may trigger a reporting obligation to ASIC under the Corporations Act.

ASX

In April 2017, the ASX published its first ASX 100 Cyber Health Check Report (ASX Report) providing insight into key issues in the identification and management of cyber risks. Whilst the NDB scheme was passed by Federal Parliament after the ASX conducted its survey, the ASX had identified the need for organisations to be on the front foot in managing cyber security and data breach risks.

From the companies surveyed, the ASX Report identified that:

- ✓ 11% of boards had a clear understanding of where the companies' key information or data assets are shared with third parties
- ✓ 35% of companies surveyed either did not have a cyber and data breach response plan in place or had developed one but not tested it to ensure it was robust enough
- ✓ 29% are confident that management can detect, respond to, and manage an incident with minimal impact on the business.

APRA

The focus on the need of RSEs to conduct Operational Due Diligence on investment managers has been on the forefront of the industry's focus following the release of the AIST Guidance note on Operational Due Diligence requirements.

It reminded RSEs of the importance of ensuring that the investment managers they engage have sufficient risk management systems, IT systems and business continuity systems in place to address cyber incidents, including data breaches.

AICD

In its latest Essential Director Update: 17, the AICD emphasised the importance of Directors and Officers understanding their compliance obligations around privacy. In the context of a discussion of the challenges posed by rapid technological developments, the AICD observed that: "Boards need to carefully assess how their organisations are structured and resourced to have a robust understanding of the regulatory frameworks and stakeholder expectations around data privacy and protection".

When discussing the NDB Scheme and the legal obligations impacting upon organisations, the AICD states: "*Company directors can use this [the NDB Scheme] as an opportunity to identify and manage the key data assets of the organisation, ensuring appropriate controls are in place. Further, it provides organisations with the opportunity [so it] can engage with customers and espouse their online trust credentials*".

Having an established Privacy Program in place, including policies and procedures to comply with the NDB Scheme will not only minimise the effects of a data breach if it occurs but will also reduce the need to rely on an insurance policy, if you have one.

Any measure taken by an organisation to improve customer engagement and trust in how it handles personal information should be embraced by Boards and may even lead to increased stakeholder returns.

4. Where do you sit on the compliance spectrum?

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 a policy. Employees need to understand how 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.

As explained in the May Paper, 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, and the looming February 2018 deadline highlight the need for organisations to have implemented their Privacy Programs as required by the 13 APPs if they have not done so already. However, in reality, we understand there is a broad spectrum of privacy compliance amongst organisations.

At one end of the compliance spectrum are organisations who have taken simplified steps to comply with the 2014 changes. This may mean having a simplified Privacy Policy explaining how it manages personal information, but not having additional policies or procedures in place to manage the personal information properly in accordance with the APPs.

At the other end of the compliance spectrum are organisations who have developed and implemented multiple and detailed policies, procedures registers and training materials and information which form a Privacy Program. Organisations in this category are in a good position to prepare themselves for the NDB Scheme requirements.

If you are one of the many organisations who do not have a Privacy Program in place, or even a Privacy Policy that supports your public privacy policy, 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 financial and reputational consequences for your organisation.

Regardless of which category of the spectrum your organisation falls in, the next section of this paper will provide practical steps for you to take now to help prepare for the NDB Scheme.

5. Practical steps to assist compliance by February 2018

Here's a list of things to do to ensure that your organisation is prepared for compliance with the NDB Scheme.

Task	Completed
Document a Privacy Program (why, what, how, who, when)	✓
Appoint a Privacy Officer	✓
Conduct a Personal Information Management Audit to test the security of personal information protection processes and procedures	✓
If you are a Credit Provider, document a Credit Reporting Policy	✓
Ensure all Information Collection Forms, such as client onboarding forms, include a Privacy Collection Notice	✓
Ensure all direct marketing communications set out clear ''opt out'' provisions	✓
Ensure that your complaints and incident management systems are working	✓
Review your Privacy Policy to ensure it reflects your approach to managing personal information, including your use of technology to collect or hold personal information	✓
Create a Data Breach Response Plan to document how your will respond to a Notifiable Data Breach	✓
Establish a Data Breach Response Team to assist the Privacy Officer in the event of a Data Breach	✓
Train your staff on privacy issues	✓
Publish your up-to-date Privacy Policy and Credit Reporting Policy on your public website	✓
Notify key stakeholders if your Privacy Policy and Credit Reporting Policy have been updated	✓
Establish practices, systems and procedures to ensure your organisation's ongoing compliance with your privacy obligations through a Compliance Program	✓
Establish practices, systems and procedures to ensure that your Privacy Program is being effectively monitored and regularly reviewed	✓

6. Next Steps for Organisations

If an organisation has not been 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. 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.

The Boards of APP entities should be using the four months before the NDB Scheme takes effect:

- ✓ to understand their legal obligations under the NDB Scheme; and
- ✓ as an opportunity to achieve a high standard of compliance,

both of which will demonstrate to stakeholders that their organisation takes privacy and data security seriously.

7. How CompliSpace Can Help

In response to the introduction of the NDB Scheme, CompliSpace has developed a detailed suite of policies and procedures, including a DBR Plan and online training content that address the provisions under the legislation. Our Privacy Module has been updated to reflect the recent final OAIC guidance and other practical updates and additions. CompliSpace has also developed detailed online privacy training which includes information on the NDB Scheme. If you do not currently subscribe to our Privacy Module, we encourage you to contact your consultant to ascertain how we can help. Subscribers to our Privacy Module will receive the updated content directly from their consultant shortly.

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.

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.