BRIEFING PAPER

CompliSpace Update

The Opportunity to Increase Trust: Mandatory Notification of Data Breaches & Complaints Handling Update

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

School Governance
Keeping you informed

TABLE OF CONTENTS

1. Executive Summary

Privacy

- ✓ 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.
- ✓ Australian regulators beyond the Office of the Australian Information Commissioner (OAIC) such as ASIC 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 their 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 Scheme in addition to their privacy statement 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 complying with the NDB Scheme. This paper explains:

- ✓ How organisations should use recently released OAIC guidance
- ✓ How regulators like ASIC 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 Australian Institute of Company Directors (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.

Complaints

The Privacy Act is one example of a myriad of legislative sources that impose a positive obligation on schools to document and effectively implement complaints handling policies and procedures. Section 5 of this paper explains how schools must develop a well-articulated complaints handling process to comply with the APPs. There are many other sources of legislation that require schools to develop a complaints handling process including the registration requirements in every state and territory. Despite legally compelling reasons for schools to ensure they have developed and implemented effective complaints handling processes, many schools fail to do so.

The introduction of the NDB Scheme should be used by schools as impetus to review their Privacy Program but also, a review of their complaints handling policies and procedures. Undertaking a review now is especially timely given recent changes to complaints handling standards.

CompliSpace's Complaints Handling Program was developed to comply with ISO 10002-2006 *Customer satisfaction – Guidelines for complaints handling in organisations*. Our Program has recently been substantially updated and now meets the guidelines as set out in the International Standard ISO 10002:2014

Quality management – Customer satisfaction – Guidelines for complaints handling in organisations and AS/NZS 10002:2014 *Guidelines for Complaint Management in Organisations.* Both these Standards superseded ISO 10002-2006 and represent national and international benchmarks in complaints handling management. We have referred to the guidance in both 2014 Standards to prepare our updates. This is because Australian regulators including the Department of Education Services Non-Government Schools WA (DES WA) and ASIC are increasingly adopting AS/NZS 10002:2014 while ISO 10002:2014 has a commercially useful focus on how a school handles the complaints it receives about its services.

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. Although the resources remain in draft format, they are unlikely to change substantially in the final version and schools may rely on them for practical guidance. Schools should continue to monitor the OAIC website for update resource, including a final Notifiable Data Breach Notification Form once it is released.

3. Regulatory Landscape: Data Security

Regulatory convergence is becoming increasingly common in the Australian regulatory landscape. To understand how the NDB Scheme impacts your organisation beyond the Privacy Act and the OAIC we have summarised below how this requirement has been addressed by the leading Australian corporate regulator, ASIC and Australia's leading industry representative body, 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. While not every school may be subject to ASIC regulation, school boards should still be aware of the focus this national regulator is placing on this key area of corporate governance.

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.

Schools should be guided by ASIC's strategic focus to influence their own business strategy on privacy and data security. Doing so will ensure they achieve a risk and compliance culture.

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 will lead to increased trust and confidence from a school community in how the school is being operated.

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 schools 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 schools.

At one end of the compliance spectrum are schools who have only taken minimum steps to comply with the 2014 changes. This may mean having a 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 schools who have developed and implemented multiple and detailed policies, procedures, registers and training materials and information which form a Privacy Program. Schools in this category are in a good position to prepare themselves for the NDB Scheme requirements.

If you are one of the many schools 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 financial and reputational consequences for your school.

Regardless of which category of the spectrum your school may be 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 school 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 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 school'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. Managing Privacy and Complaints

An integral part of a Privacy Program is the establishment of a Complaints Handling Program. Several APPs address the need for an APP entity to have avenues for persons to contact them regarding how their personal information is being managed.

For example:

- ✓ APP 1: Open and Transparent Management of Personal Information
- ✓ APP 13: Correction of Personal Information.

In order to comply with the APPs, schools must have a well-articulated complaints handling process in relation to the collection, use and disclosure of personal information. If you are one of the schools who, due to taking minimal action in response to the 2014 Privacy Act changes, is at the dubious end of the compliance spectrum described at Section 4 of this paper, it is likely that you are also a school that does not take their complaints handling processes seriously.

However, the Privacy Act is only one source of legislation that requires school to have complaints handling policies and procedures in place. The education regulatory frameworks of state and territory governments are constantly evolving to include and enhance similar legal obligations for various aspects of a school's operations, including the regulation of international students. In addition, school regulators are now prescribing that schools must meet governance standards relating to complaints management. For example in the DES WA's Guide to the Registration Standards and Other Requirements for Non-government Schools 2017, the DES WA states that a school's complaints management system, which includes its policy and procedures as well as complaints records, will be evaluated by reference to AS/NZS 10002:2014. DES WA is following the approach of non-school regulators such as ASIC by endorsing AS/NZS 10002:2014.

Consequently, in light of the latest NDB reforms to the Privacy Act, now is the time for schools to start taking their complaints seriously and for school councils to start demanding transparency as to the numbers and types of complaints that are being received by their school.

CompliSpace has developed a Complaints Handling Program through which schools can manage privacy related complaints. There are many benefits to effectively managing privacy complaints internally, including minimising the opportunity for a complaint to be made externally to the OAIC and ensuring stakeholder confidence in the school's governance procedures.

The Complaints Handling Program previously aligned with AS/ISO 10002:2006 which has been superceded by ISO 10002:2014 and the Australian Standard AS/NZS 10002:2014. CompliSpace's updated Complaints Handling Program aligns with the principles in both AS/ISO 10002:2006 and Australian Standard AS/NZS 10002:2014.

The focus of ISO 10002:2014 on customer satisfaction is a key attribute of ISO 10002:2014, which is especially relevant to schools who have multiple stakeholders.

From a privacy perspective, receiving a complaint from a member of the school community about how their personal information is being managed will allow a school to detect and respond to flaws in their information security procedures, which may then avoid a NDB occurring.

7. Next Steps for Schools

If a school 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 a school's general approach to risk management. In order to comply with the NDB requirements, the school 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.

8. 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 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.

In response to the release of ISO 10002:2014 and AS/NZS 10002:2014 CompliSpace has updated our Complaints Handling policies and procedures to align with the key principles from both Standards. If you do not currently subscribe to our Complaints Handling Program, we encourage you to contact your consultant to ascertain how we can help. Subscribers to our Complaints Handling Program 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 and complaints handling GRC services in Australia, working with leading non-government schools 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.