Australia – Notifiable Data Breach Legislation

DISCUSSION DOCUMENT

NICK VUJCICH

1 Table of Contents

2 Introduction

This document has been written to support Datavator customers operating in Australia to understand the changes to the Notifiable Data Breach Act and the impact this could have on their organisation in terms of financial risk and the requirements that an organisation should have in place to comply with this legislation.

3 Intended Audience

This document is intended for Senior Management and Security teams that are required to support a risk-based approach to Cyber security

4 Executive Summary

- The Australian Notifiable Data Breaches (NDB) scheme requires businesses to notify the Office of the Australian Information Commissioner (OAIC) and affected individuals in the event of a data breach involving personal information.
- To comply with the NDB scheme, businesses should take a risk-based approach to cybersecurity and develop a data breach response plan. They should also take proactive steps to protect personal information, such as implementing appropriate technical and organizational measures, training employees, and regularly reviewing and updating their privacy and data protection policies.
- ISO 27001 is a widely recognized information security management standard that can help businesses identify and manage risks related to the security of their information assets. Implementing ISO 27001 can help businesses meet the requirements of the NDB scheme and improve their overall information security posture.
- Executives can be held liable under the NDB scheme and could face fines, penalties, and reputational damage in the event of a data breach. It is therefore important for executives to prioritize information security and privacy and ensure that their organizations are taking appropriate steps to protect personal information.

5 What is the Notifiable Data Breach Act

The Australian Breach Notification legislation, known as the Notifiable Data Breaches (NDB) scheme, requires businesses to report data breaches that involve the personal information of individuals to the Office of the Australian Information Commissioner (OAIC) and the affected individuals. The scheme applies to businesses and organizations covered by the Privacy Act 1988, including businesses with an annual turnover of more than $3 million, credit reporting bodies, and health service providers.

Under the NDB scheme, a data breach is defined as the unauthorized access or disclosure of personal information, or loss of personal information. If a business becomes aware of a data breach that is likely to result in serious harm to any affected individuals, it must notify both the OAIC and the individuals whose personal information has been compromised as soon as practicable. Serious harm can include financial, reputational or other types of harm.

Failure to comply with the NDB scheme can result in significant consequences for businesses. The OAIC can investigate and take enforcement action against businesses that do not comply, which can result in fines of up to the maximum penalty for a serious or repeated interference with privacy is now the greater of A$50 million, three times the benefit of a contravention, or (where the benefit can't be determined) 30% of domestic turnover and up to $420,000 for individuals. Additionally, businesses that do not comply with the NDB scheme may also face reputational damage and loss of customer trust, which can have significant costs outside of the initial fine.

To comply with the NDB scheme, businesses should have a data breach response plan in place that outlines the steps to take in the event of a data breach, including assessing the nature and extent of the breach, containing the breach, and notifying affected individuals and the OAIC as required. Businesses should also take proactive steps to protect personal information, such as implementing appropriate technical and organizational measures, training employees, and regularly reviewing and updating their privacy and data protection policies.

6 Areas of Change Post the Optus Breach

- The Australian Parliament has passed privacy reforms under the Privacy Legislation Amendment (Enforcement and Other Measures) Bill 2022 (Cth) that introduce new privacy penalties. The maximum penalty for a serious or repeated interference with privacy is now the greater of ;
  - A$50 million,
  - three times the benefit of a contravention
  - or (where the benefit can't be determined) 30% of Australian Turnover.
- Australian privacy laws will now apply to organizations doing business in Australia, whether or not personal information is collected in Australia.
- The Office of the Australian Information Commissioner (OAIC) will have a broader set of regulatory tools and information-gathering powers to work with, and information-sharing will be improved within the OAIC and among regulators (including foreign regulators).
- The new penalties are intended to create incentives for strong data security safeguards and are a clear message from the Australian Government that penalties for privacy breaches are not "simply the cost of doing business".
- Businesses that do not comply with the NDB scheme may face reputational damage and loss of customer trust, which can have significant costs outside of the initial fine, including increased insurance costs and legal fees associated with investigations, notifications, and response to the data breach.
- These reforms are only the first tranche of a comprehensive review of Australia's privacy laws for the digital era. The final report on the review will be delivered to the Government by the end of this year, and there is ample room for clarification on how the new penalties will apply.
- Businesses should take a risk-informed approach to cybersecurity, actively manage privacy risks, invest in harm reduction, and understand and plan for financial exposure.
- The Australian Senate has called on the Government to clarify key definitions, develop a tiered penalty regime, issue guidance material, and consider the adequacy of current resourcing and staffing levels at both the Office of the Australian Information Commissioner and the Australian Cyber Security Centre.

7 Business Requirements

The Australian Notifiable Data Breaches (NDB) scheme requires businesses to notify the Office of the Australian Information Commissioner (OAIC) and affected individuals in the event of a data breach involving personal information. Here's an executive summary of what this means for your business:

1. If your business experiences a data breach that is likely to result in serious harm to any affected individuals, you must notify both the OAIC and the affected individuals as soon as practicable.
2. You must conduct an assessment of the data breach, including the nature of the data involved and the risks to affected individuals.
3. You must take steps to contain the breach and prevent further unauthorized access or disclosure of personal information.
4. You must develop a data breach response plan and provide ongoing employee training on data protection and privacy.

7.1 Practical Steps

1. Develop a data breach response plan: Develop a plan for how your business will respond in the event of a data breach, including steps for identifying and containing the breach, assessing the risks to affected individuals, notifying affected individuals and the Office of the Australian Information Commissioner (OAIC), and reviewing and updating your privacy policies and procedures.
2. Conduct a privacy impact assessment: Conduct a privacy impact assessment to identify the personal information your business collects, uses, and discloses, and to assess the risks to that information.
3. Implement appropriate technical and organizational measures: Implement appropriate technical and organizational measures to protect personal information from unauthorized access, disclosure, loss, or misuse. This may include measures such as encryption, access controls, and employee training.
4. Train employees: Train employees on your business's privacy policies and procedures, including how to identify and report data breaches, and how to respond to customer inquiries and complaints.
5. Review and update privacy policies and procedures: Regularly review and update your business's privacy policies and procedures to ensure they are up-to-date and reflect changes in your business operations, technologies, and legal requirements.
6. Conduct regular security audits: Conduct regular security audits to identify vulnerabilities in your business's information systems and to ensure that appropriate security controls are in place.
7. Monitor for data breaches: Monitor your business's information systems for data breaches, and implement appropriate procedures for identifying and containing breaches when they occur.

By taking these steps, businesses can help to minimize the risk of data breaches and ensure that they are able to respond effectively in the event of a breach. They can also help to demonstrate compliance with the requirements of the NDB scheme, and avoid the significant consequences of non-compliance.

8 Consequences of non-compliance:

The OAIC can investigate and take enforcement action against businesses that do not comply, which can result can now reach the greater of A$50m, three times the benefit of a contravention, or (where the benefit can't be determined) 30% of domestic turnover and up to $420,000 for individuals.

Businesses that do not comply with the NDB scheme may also face reputational damage and loss of customer trust, which can have significant costs outside of the initial fine.

Additionally, customers have a private right of action to sue businesses for damages resulting from a data breach.

8.1 Costs outside of the initial fine:

- Reputational damage and loss of customer trust.
- Increased insurance costs.
- Legal fees and costs associated with investigations, notifications, and response to the data breach.

- Costs associated with implementing measures to prevent future data breaches, such as employee training and technology upgrades.
- Remediation of customers costs for management of personal data such as reissuance of government identity, credit cards, credit scoring monitoring

9 Executive and Senior Management Risk

Executives and senior managers of a business may be held liable under the Notifiable Data Breaches (NDB) scheme if the business fails to comply with the requirements of the scheme. In particular, the Privacy Act 1988 allows the Office of the Australian Information Commissioner (OAIC) to take enforcement action against a business, which may include taking legal action against individual executives and managers.

Under the NDB scheme, a business that experiences a data breach that is likely to result in serious harm to any affected individuals is required to notify both the OAIC and the affected individuals as soon as practicable. If the business fails to comply with this requirement, the OAIC can investigate the breach and take enforcement action, which may include imposing fines and other penalties. In serious cases, the OAIC may also take legal action against individual executives and managers who are responsible for the breach.

In addition to enforcement action by the OAIC, customers may also have the right to sue a business for damages resulting from a data breach. The Privacy Act 1988 includes a private right of action that allows individuals to sue businesses for breaches of privacy, including breaches of the NDB scheme. To be successful in such a claim, the individual would need to demonstrate that the business breached its obligations under the NDB scheme, and that this breach caused them to suffer harm or loss.

It's important to note that the potential liability of executives and managers under the NDB scheme and the Privacy Act 1988 emphasizes the importance of establishing a strong culture of privacy and data protection within a business. Executives and managers should take an active role in ensuring that the business complies with its obligations under the NDB scheme and other relevant data protection laws, and that appropriate measures are in place to protect personal information.

9.1 Risk of Jail for Executives

In Australia, executives can face criminal liability if they are found to have intentionally or recklessly contravened the Privacy Act 1988 (Cth), which requires organizations to take reasonable steps to protect personal information they hold. If an executive is found to have acted with intent or recklessness, they may be subject to fines and even imprisonment.

However, it is relatively rare for executives to face criminal charges in connection with a data breach. Prosecutions are typically pursued only in cases of severe or repeated violations of privacy laws, or where the executive's actions were particularly egregious.

In practice, executives are more likely to face civil penalties or compensation claims if their organization experiences a data breach. They may also face consequences for their reputation and career if the breach results in significant harm to individuals or the organization.

10 Useful Information

10.1 Link to OAIC Report to June 2022

https://www.oaic.gov.au/__data/assets/pdf_file/0020/23663/OAIC-Notifiable-Data-Breaches-Report-Jan-Jun-2022.pdf

10.2 Further information

https://www.upguard.com/blog/australian-data-breach-stats

https://www.consultancy.com.au/news/6560/will-australia-see-its-first-1-billion-data-privacy-fine-in-2023

https://thehackernews.com/2022/11/australia-passes-bill-to-fine-companies.html

https://www.upguard.com/blog/biggest-data-breaches-australia

https://www.webberinsurance.com.au/data-breaches-list#twentytwo

https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-statistics/notifiable-data-breaches-report-january-june-2022

https://www.dataprotectionreport.com/2023/02/privacy-act-review-report/