Notifiable Data Breaches: What You Need to Know

What is the Privacy Amendment Act?

The Privacy Amendment (Notifiable Data Breaches) Act 2017 has been enacted by the Australian government to amend the Privacy Act 1988, the original law regulating the handling of individuals' personal information. The act expands upon the scope of personal data privacy for Australian residents and applies fully as of 22 February 2018.

The Notifiable Data Breaches (NDB) scheme introduces an obligation to notify individuals whose personal information is involved in a data breach that is likely to result in harm to those whose data was compromised. The notification must include recommendations about the steps individuals should take in response to the breach. The Australian Information Commissioner must also be notified of eligible data breaches.

Agencies and organisations are required by the Privacy Act 1988 and its 2017 amendment to take steps to secure certain categories of personal information that can easily identify an individual. This includes Australian Government agencies, business and non-profit organisations with an annual turnover of $3 million or more, credit reporting bodies, health service providers, and TFN recipients, among others.

"As a globally active organization, Therefore Corporation welcomes the new regulation as a step in the right direction towards strengthening personal privacy rights."

How Therefore™ can help:

The Privacy Amendment (Notifiable Data Breaches) Act 2017 requires significant effort and investment in data security and protection by any affected entity. By relying on the concepts of Privacy by Design and Privacy by Default, Therefore™ offers an ideal solution towards compliance.

Therefore Corporation strives to help you achieve compliance by offering an information management solution that allows you to store, find, and catalog the personal data retained by your organisation and create a more secure data environment. Furthermore, Therefore™ offers resources that simplify the monitoring and management of the personal data you retain within the system, and provides tools to help you meet the regulation's reporting and assessment requirements.

However, based on the broad scope and nature of the Privacy Act and the NDB scheme, it is important to recognize that compliance goes beyond software. Compliance is the result of a combination of sound data protection policies, procedures, training, and reporting. Therefore™ can help your organisation achieve these results, and thus compliance, by providing tools which make it easier for you to discover, manage, secure, and report on the personal data your organization retains.

How Therefore™ helps at a glance...

- Store, find, and catalog the personal data retained by your organization
- Simplify the monitoring and management of personal data
- Create a more secure data environment
- Tools to help meet reporting and assessment requirements

Therefore™
PEOPLE PROCESS INFORMATION

How do I get started?

The Privacy Act has many requirements about how your organisation can collect, store, and use personal information. These include:

- How you identify, store, and secure the personal data in your systems
- How you accommodate requirements for data transparency
- How you detect and report personal data breaches
- How you train privacy personnel and employees
- And more

Since so much preparation is involved for adherence to this new regulation, Therefore Corporation recommends getting a head start on compliance preparations. Start reviewing your data management practices and policies as soon as possible. Non-compliance with the Privacy Act and the NDB scheme has the potential to cause serious financial or reputational harm to your organisation; sanctions could include anything up to $2.1 million. However, proof of a robust set of security provisions in place and the response time to reporting a data breach incident can be taken into consideration when the authorities are evaluating the situation.

You should start on the path to compliance by focusing on the following key areas:

DISCOVER: Prevention and Preparation

- Identify the type of personal data your organisation collects and how you retain it
- Perform a risk assessment and threat analysis to get an idea of where you currently stand
- Appoint the appropriate personnel to preside over data handling initiatives
- Train your staff to ensure data handlers are aware of the new regulation and how to adhere to it

MANAGE AND SECURE: Security Implications

Implement policies and tools to manage how the personal data you retain is managed and accessed:

- Prevent non-authorized personnel from accessing personal data

Within Therefore™:

- Check your permission settings to ensure only authorized users have access to personal data

- Make sure you have enabled backup drives, storage and retention policies, and migration schedules to retain data properly
- Set retention policies to delete outdated information (after the retention period specified by applicable local laws)

REPORT: Data Breaches and Actions to Take

Implement policies and procedures for dealing with and reporting data breaches:

- Maintain meticulous records of your organisation's security implementations
- Establish a procedure or strategy for effectively communicating a breach to the authorities as soon as possible

Within Therefore™:

- Configure Therefore™ Audit Trail to log actions taken by system users, and regularly review the logs for signs of suspicious activity.
- Store documentation related to your organisation's security implementations in Therefore™, and build a workflow around the process of organisational review.

REVIEW: Privacy Policies and Access to 'Personal Information' Requests

Implement privacy policies and procedures:

- Establish a protocol or procedure for handling 'personal information' requests
- Regularly keep track of data protection regulations to ensure that business processes remain in-line with the law
- Update organisational privacy policies

Within Therefore™:

- Create a workflow for handling personal information requests to make the process fully documented and traceable
- Consider organizing personal data into logical groupings that make it easy to respond to personal information requests
- Always install the latest recommended patches and updates to ensure your system remains secure