



# Mandatory Data Breach Notification:

## Helping organisations to be data breach secure

### What is the new privacy law?

The Notifiable Data Breaches (NDB) scheme requires organisations to notify the Office of the Australian Information Commissioner (OAIC) and the affected individuals of an eligible data breach as soon as practical. If the data breach is likely to result in serious harm, organisations must conduct an assessment within 30 days. This may be as few as one record.

If the breach is eligible, a data breach notification is deemed compulsory unless it would impact upon a law enforcement investigation or has been determined by the regulator to be contrary to public interest.

### Who does the legislation apply to?

The new law applies to public and private organisations that are already subject to the Privacy Act – this includes Australian Government agencies (excluding state and local government) and all businesses and not-for-profit organisations with an annual turnover more than \$3 million. However organisations or individuals that trade in personal information (e.g., health records, credit data, etc.) regardless of their revenue, are NOT exempt.

### What is a data breach?

A data breach occurs when personal information that an entity holds is subject to unauthorised access or disclosure, or is lost.

The NDB scheme requires organisations to notify individuals and the OAIC about eligible data breaches. The OAIC identifies an eligible data breach as:

- When there has been unauthorised access to, or unauthorised disclosure of, personal information held by an entity (or information is lost in circumstances where unauthorised access or disclosure is likely to occur).
- It is likely to result in serious harm to any of the individuals to whom the information relates.
- The organisation has not been able to prevent the likely risk of serious harm with remedial action.

Relevant data can include sensitive information such individual's health records, Medicare card, driver licence, passport details, credit information, tax file number and other financial information.

A real risk of "serious harm" can include physical, psychological, emotional, economic and financial harm, and also includes serious harm to reputation.

**Having a comprehensive cyber risk mitigation strategy in place is your first line of defence in limiting the damage that a data breach could have.**



### What are the penalties?

Under the new laws, where a breach has occurred and is deemed "a serious or repeated or repeated interference with privacy", penalties including fines of up to \$420,000 for individuals and \$2.1 million for organisations could apply.

### Risk transfer solution

Cyber insurance provides comprehensive cover for first and third party exposures in relation to any cyber or privacy event that impacts your business. It provides your business with a structured crisis response plan to mitigate further loss and assists with returning to 'business as usual'.



### What is covered?

#### ► First party

- Business interruption (loss of income and extra expenses)
- Costs to restore/recreate data
- Notification costs & credit monitoring services including identity theft management
- Forensic and accounting investigation expenses
- Cyber extortion costs
- Crisis communication/ public relations costs
- Legal costs assisting with privacy notification/compliance response

#### ► Third party

- Defamation claims
- Infringement of privacy and intellectual property claims
- Claims arising from network security failures
- Claims as a result dissemination of confidential information or damage to third-party systems
- Legal defence costs
- Privacy breach regulatory proceedings and investigations
- Fines & penalties



## Contacts

### **Fergus Brooks**

*National Practice Leader, Cyber Risk*

+61 2 9253 7835

fergus.brooks@aon.com

### **Michael Parrant**

*Cyber Insurance Practice Leader*

+61 3 9211 3485

michael.j.parrant@aon.com

[aon.com.au/cyber](https://aon.com.au/cyber)

### **About Aon**

Aon is the leading global provider of risk management, insurance and reinsurance brokerage, and human resources solutions and outsourcing services. Through its more than 66,000 colleagues worldwide, Aon unites to empower results for clients in over 120 countries via innovative and effective risk and people solutions and through industry-leading global resources and technical expertise. Aon has been named repeatedly as the world's best broker, best insurance intermediary, reinsurance intermediary, captives manager and best employee benefits consulting firm by multiple industry sources. Visit [aon.com](https://aon.com) for more information on Aon and [aon.com/manchesterunited](https://aon.com/manchesterunited) to learn about Aon's global partnership and shirt sponsorship with Manchester United.

**[aon.com](https://aon.com)**

© Aon plc 2018. All rights reserved.

The information contained herein and the statements expressed are of a general nature and are not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information and use sources we consider reliable, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.