fordham

What is the new notifiable data breaches scheme?

By Fordham
4 April 2018

Scan the media on any given day, and chances are you will find another story relating to privacy and the impact of security breaches. Indeed, likely you have been the victim of a data breach (albeit minor) yourself. New privacy laws came into effect earlier this year to help protect

personal data, however this may impact the way you and your business need to report any data breaches.

WHAT IS A DATA BREACH?

Examples of data breaches range from business scenarios that are unfortunately all too common:

- Personal information is mistakenly provided to the wrong person
- Data or records containing customers' personal information is lost
- To the actively malicious:
- A database containing personal information is hacked
- A cyber attack resulting in personal information being disclosed

WILL THE SCHEME IMPACT MY BUSINESS?

The new Notifiable Data Breaches (NDB) came into effect on 22 February 2018 and applies to all businesses, agencies and organisations with existing personal information security obligations under the Privacy Act 1988. **This means that if you're a business or not-for-profit organisation, with an annual turnover of $3 million or more, you need to comply with the new scheme.**

WHAT IS THE NOTIFIABLE DATA BREACHES SCHEME?

The scheme effectively mandates the reporting and notification process of any data breaches, with businesses now required to report any data breach "likely to result in serious harm" to an individual. Note that "serious harm" is not defined in the Act. In the context of a data breach, it may include serious physical, psychological, emotional, financial, or reputational harm.

HOW DO I REPORT A DATA BREACH?

Breaches need to be reported to the Office of the Australian Information Commissioner (OAIC) and the impacted individuals as soon as possible. The notification must include the following information:

- Identity and contact details of the organisation
- Description of the data breach
- The kind of information concerned
- Recommendations about the steps individuals should take in response to the breach

HOW CAN I ENSURE MY BUSINESS IS COMPLIANT?

We recommend businesses develop their own procedures for assessing a suspected data breach. You should consider:

- Reviewing current information security practices, procedures and systems to ensure they are adequate
- Taking steps to ensure all security software and controls are up to date

- Removing access to data from people who do not need it as part of their role
- Preparing a data breach response plan (or updating a current plan) to enable a quick response to a suspected breach
- Providing training to relevant staff as to what they need to do regarding reporting and responding

WHERE CAN I GO TO FOR HELP IN THE EVENT OF A BREACH?

The Australian Taxation Office (ATO) can help you in the event of a data breach and may apply measures to protect your business, staff and clients. More information on data breaches and support is available on both the ATO and OAIC websites.

WHAT HAPPENS IF I FAIL TO COMPLY?

If you fail to comply with the new scheme and don't disclose a data breach then penalties may apply. **Penalties for not notifying affected parties and the OAIC of a data breach include fines of up to $420,000 for individuals and $2.1 million for organisations.**

WHAT'S NEXT?

We recommend all clients to review their practices, procedures and systems for securing personal information in order to comply with these new provisions. Should you require further advice on data breach reporting and how these changes may affect you, please contact your Fordham Partner for a confidential discussion.