ARE YOU READY FOR THE MANDATORY DATA BREACH NOTIFICATION LAW?

The federal data breach notification law comes into force on 22 February 2018. The law makes it mandatory for businesses who are bound by the Privacy Act to self-report certain types of data breaches. Here are ten things you need to know about the new law.

1 **Mandatory data breach notification is law**

The data breach notification requirement is not a recommendation or a code or a guideline – it's law. It comes into full force on 22 February 2018. Applicable businesses must comply with the law from that date.

2 **The law applies to certain businesses**

The data breach notification law applies to businesses (and not-for-profits) who are bound by the *Privacy Act 1988* (Cth). This includes businesses who have an annual turnover of $3 million or more, health service providers, credit providers, credit reporting bodies and businesses who trade in personal information.

3 **Certain data breaches must be notified**

Where there is unauthorised access, unauthorised disclosure or loss of personal information that is likely to result in serious harm to a person, a business must notify the affected person/s and the Australian Information Commissioner. The new law makes notification mandatory.

4 **Suspected data breaches must be investigated**

If a business suspects a data breach has occurred, it must investigate to determine if the data breach needs to be notified. The new law says that businesses can't ignore suspected data breaches or turn a blind eye.

5 **"Serious harm" is not just about credit card numbers**

The key trigger that makes a data breach notifiable is that it is likely to result in "serious harm" to a person. Serious harm can include financial, physical, psychological, emotional and reputational harm.

6 **Notification is not just a form-filling exercise**

A data breach notification must provide not only the details of the data breach but also recommendations on what affected people should do to minimise the risk of serious harm. Providing recommendations may require getting specialist advice (e.g. from IT, security, fraud experts).

PHONE: 1300 158 788 / +61 3 9866 8850
EMAIL: DATABREACHLAWS@COOPERMILLS.COM.AU

www.coopermills.com.au

CooperMills LAWYERS

7 **Effective remedial action removes the need for notification**

A business does not need to notify a data breach if it takes timely remedial action that prevents the likelihood serious harm. For example, the timely remote deletion of data from a lost laptop may be remedial action that prevents the risk of serious harm.

8 **Businesses need to talk to their outsourced providers**

Outsourcing providers (e.g. outsourced billing, support or marketing providers) are likely to hold a business' data. Businesses and their outsourced providers need to work out the responsibilities, arrangements, procedures and liability for dealing with a data breach.

9 **Non-compliance can have legal consequences**

Non-compliance with the data breach notification law can have serious consequences. The potential consequences of not complying with the data breach notification law include regulatory investigation, orders to pay compensation and substantial civil penalties.

10 **Businesses need to prepare for the law now**

If the mandatory data breach notification law applies to your business, you should prepare for it now. Having the necessary knowledge and understanding about the new law and how it works is essential.

GETTING READY
FOR THE DATA BREACH NOTIFICATION LAW

The data breach notification law comes into force on **22 February 2018**. Cooper Mills Lawyers has prepared a number of expert guides to help you plan for and comply with the new law. To get a copy of these guides, contact Peter Moon, Erhan Karabardak or Victor Ng on **1300 158 788** or email **databreachlaws@coopermills.com.au**.

GUIDE TO UNDERSTANDING THE DATA BREACH NOTIFICATION LAW

A short but comprehensive guide on the mandatory data notification law. Essential reading for business executives, employees and contractors who need to understand the new law. Plain English guaranteed!

GUIDE TO PREPARING FOR THE DATA BREACH NOTIFICATION LAW

A step-by-step guide on what you can do to prepare for the new law, including how to audit your business data and assess risk, roles and responsibilities of a data breach response team and a data breach response plan template.

GUIDE TO RESPONDING TO A DATA BREACH

A step-by-step guide on how to respond to a data breach under the data breach notification law, including a response flowchart and the key self-reporting obligations and notification forms.