IAB AUSTRALIA REGULATION UPDATE:

NEW MANDATORY DATA BREACH NOTIFICATION LAWS

From 22 February 2018, the Privacy Act 1988 (Cth) will include a mandatory data breach notification scheme. This means you will have to alert authorities and all affected individuals about any 'eligible data breach' which takes place in your company.

1. Will the new mandatory data breach laws affect my company?

Yes, if you are a business with an annual turnover of more than $3 million; or if you are a business with an annual turnover less than $3 million but you sell or purchase personal information as part of your operating processes.

2. What do you need to do to prepare for the new laws?

You should familiarise yourselves with this guidance on what the laws mean for your companies, and also take steps now to ensure your practices and processes protect you in the occurrence of a data breach and allow you to meet any new obligations.

3. What do I need to do if I discover a data breach?

The Mandatory Data Breach Notification scheme will require you to notify the Office of the Australian Information Commissioner (OAIC) (which can be done via email) and all affected individuals as soon as practicable in the event of a data breach.

The core driver of this new scheme is to allow individuals consumers to take any steps they need to protect themselves if a company compromises their personal information.

4. If I discover a data breach but decide the information at risk of breach was encrypted, do I need to report it? When is it mandatory that I report the breach?

An eligible data breach occurs when personal information of and individual/consumer has been viewed, stolen or used by an individual unauthorised to do so. This may occur in your company by accident (e.g loss of a work iPhone or tablet in a public space) or may occur by deliberate attempts to illegally obtain protected information. (e.g. hacking, systems compromised).

If the data breach is likely to lead to a risk of serious harm, then you need to report it.

You can determine the test for serious harm by reference to a number of factors in Part IIIC of Privacy Amendment (Notifiable Data Breaches) Act 2017.

5. Exceptions to Data Breach Notification requirement

If a company takes remedial action to ensure no serious harm to any individual is likely to occur before any serious harm is actually caused to any individual by the data breach there is no requirement to notify.

Clearly, this exception, demonstrates the value of preparing ahead, and implementing policies to prepare for any potential compromise of your company systems. At a minimum, as your company is subject to these laws, you should have in place internal guidance on what steps an employee should take if a data breach is discovered regardless of whether the breach has occurred as the result of inadvertent misadventure by one of your staff or deliberate attack by an external entity.

6. What kind of penalties and damages can apply?

Penalties vary depending on the seriousness of the breach. A failure to follow notification steps prescribed by the law, will fall under the existing penalties listed in the Privacy Act. The range of penalties which might apply to your company include investigation by authorities or, in the case of very serious non-compliance with breach notifications, your company can face penalties of up to $2.1m.

In addition, if there is a complaint/class complaint, where you are found to have breached privacy law (i.e. any of the Australian Privacy Principles or failure to notify on eligible data breach, for example) damages can be awarded and are usually in the range of $10,000 to $15,000 per successful complainant (e.g. for a 1,000 affected individuals, possible damages of $10m to $15m).

7. EY Breach Notification Guide

Attached is a guide to assist you, from 22 February 2018, to determine when you might have an ‘eligible data breach’ which requires notification to the Privacy Commissioner and all affected individuals.

DOWNLOAD THE DATA BREACH FLOW CHART HERE.