Are you ready for the new Australian data protection regulations?

On 13 February 2017, the Federal Government passed the Privacy Amendment (Notifiable Data Breaches) Bill 2016, which is set to come into effect within a year.

The scale of the changes means organisations should start their preparations now.

The law aims to incentivise the holders of data to adequately secure or dispose of that information. It also allows individuals whose personal information has been compromised by a breach to take remedial steps to lessen the adverse impact that might arise from the breach. As a result, a number of new measures will be introduced that will require attention.

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.

What is a data breach?

A data breach is defined as a situation where:

- there has been unauthorised access to, or unauthorised disclosure of, personal information about one or more individuals, or
- such information is lost in circumstances that are likely to give rise to unauthorised access or unauthorised disclosure.
- there is a likely risk of serious harm to any of the affected individuals as a result of the unauthorised access or unauthorised disclosure.

Relevant data can include data such as personal information, credit information, tax file numbers.

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

Data breach response plan

In order to adequately comply with the new requirements it is essential to have a data breach response plan in place. This should address the following:

At what point do we need to inform the OAIC?

Within 30 days after the entity has become aware that there are reasonable grounds to believe that there has been an eligible data breach.

What information must be included in the notification?

- the identity and contact details of the entity
- a description of the serious data breach
- the kinds of information concerned, and
- recommendations about the steps that individuals should take in response to the serious data breach.

Where do we access legal advice?

Organisations may be able to get certain firms pre-approved with their cyber insurers

How will we independently investigate a cyber–attack or incident?

Consider how you will demonstrate that you took suitable action to implement appropriate technical and organisational measures to ensure compliance.

What is our media strategy?

The reputational costs can be significant, ensure you have a communications plan in place to handle the situation in a timely manner to pro-actively engage your clients and limit damage.

Key implications

These are some of the most significant changes that will be introduced:

Compulsory regulatory notification

In the event of a data breach, the organisation has a duty of notification to the Office of the Australian Information Commissioner (OAIC) and the affected individuals of an eligible data breach within 30 days after the entity has become aware that there are reasonable grounds to believe that there has been an eligible data breach.

This is a game changer. Currently, whilst organisations subject to the Privacy Act are 'encouraged' to notify OAIC in the event of a data breach, they have no legal obligation to do so. This will make the response to these incidents compulsory and time critical.

The amount of data may be as little as one of the above records.

Notification is deemed compulsory unless it would impact upon a law enforcement investigation or was determined by the regulator to be contrary to the public interest.

Penalties

Under the new laws, where an organisation has committed "serious or repeated non-compliance with mandatory notification requirements" they could be faced with penalties including fines of up to $360,000 for individuals and $1.8 million for organisations.

However, a significant data breach to your organisation can be financially crippling. Resultant costs could range from business interruption, incident response, third party claims and legal costs, to customer notification expenses and damage to data.

These financial implications will require a systematic change of attitude for many organisations, with cyber risks and data security elevated to boardroom level.

Preparing for the new regulations

With these significant changes set to be introduced, it is important to start considering them as soon as possible. We recommend appointing a steering committee to ensure that all the implications of the new regulations are fully understood and existing systems and processes are adapted to reflect the new requirements.

Running a full risk assessment can be a useful exercise. This will highlight where there are any potential issues and enable you to take action now to avoid problems when the regulations are introduced.

Insurance could be a consideration. Aon, together with insurers, has created cyber policies to address this exposure. As well as covering losses that may be incurred, this also ensures the right expertise is available when a data breach occurs.

Whether or not insurance is appropriate, prudent risk managers should be considering their obligations and making sure the correct processes and systems are in place ahead of the legislation coming into effect.

How we can help

We can help you understand the implications of this legislation, and what is means for your organisation. This may include reviewing your organisations cyber risk profile and considering your cyber insurance and incident response plan. If you would like to discuss further please contact our Fergus Brooks, our National Practice Leader for Cyber Risk.

Fergus Brooks
National Practice Leader,
Cyber Risk
+61 2 9253 7364
fergus.brooks@aon.com