Notifiable Data Breach Scheme

A data breach happens when personal information is accessed or disclosed without authorisation or is lost. Australia's Mandatory Data Breach reporting law, known as the Notifiable Data Breach (NDB) Scheme came into effect on 22 February 2018.

Those businesses that comply must notify affected individuals and the government when a data breach involving personal information is likely to result in serious harm. At BES, we want to keep you aware and compliant.

1 WHO NEEDS TO COMPLY?

If you fall into one of the following categories, then you not only have to comply with the Privacy Act, but now you also need to comply with the NDB Scheme.

- Australian Government agencies
- credit reporting body
- health service providers
- TFN recipient (someone holding a Tax File Number in your systems)
- business or non-profit organisation with an annual turnover of more than $3 million

DID YOU KNOW:

Under the new laws, a business is required to notify those at risk within 30 days of a breach.

2 WHAT IS AN ELIGIBLE DATA BREACH?

An eligible data breach is one in which there is unauthorised access, disclosure or loss of personal information held by an entity and that access, disclosure or loss is "likely to result in serious harm to any of the individuals to whom the information relates".

In this situation, "serious harm" includes physical harm, financial/economic harm, emotional harm (e.g. embarrassment and humiliation), psychological harm (e.g. marginalisation and bullying) and reputational harm.

If a data breach occurs and the data could lead to the type of harm mentioned, it is your legal obligation to comply with the new NDB Scheme laws.

3 WHAT ARE THE NEW OBLIGATIONS?

If the organisation incurs an "eligible data breach", within 30 days it must notify individuals whose personal information is likely to result in serious harm due to the breach. The organisation is also obligated to alert the Australian Information Commissioner of the eligible data breach.

BES Information Technology Systems
Established 1988

16 Cinderella Drive,
Springwood QLD
07 3340 5555
sales@bes.com.au
www.bes.com.au

Your security is our priority

We offer security audits and security awareness training to help you stay safe. Contact us today.

4 WHAT IF YOU FAIL TO REPORT?

If you fail to report an eligible breach of data, both individuals and the business itself will face serious consequences. Individuals will face penalties up to $360,000 and $1.8 million for organisations.

5 HOW CAN YOU PREPARE?

- Seek legal advice to ensure that you are fully aware of your obligations
- Secure your networks and protect against viruses, spyware, and other malicious code
- Establish or review IT security practices and policies to protect sensitive information
- Educate employees about cyberthreats and hold them accountable
- Be prepared with procedures and protocols in place should a data breach occur

If you are unsure of where to start and need to chat with someone who understands the scope of this law, contact BES today.

Our team is on the front line of cyber security every day and can help you assess, identify and remediate security challenges.

THINGS YOU CAN DO TO AVOID A BREACH:

Review your cyber security protocol with a comprehensive audit from our team.

Ensure your staff are appropriately trained in current cyber security protocols.

Keep your security software, like Anti-Virus, Email Filtering and Multi-Factor Authentication up to date - crucial elements of your business continuity plan.

BES Information Technology Systems
Established 1988

16 Cinderella Drive,
Springwood QLD
07 3340 5555
sales@bes.com.au
www.bes.com.au

Your security is our priority

We offer security audits and security awareness training to help you stay safe. Contact us today.