Cyber checklists

NDB SCHEME

wotton kearney

A founding member of LEGALIGN GLOBAL

Privacy for Small Businesses – Does the NDB Scheme Apply to Me?

For the Notifiable Data Breach Scheme (NDB Scheme) to apply to your business, you must be covered by the Privacy Act 1988 (Cth). Only certain businesses are covered by the Act and subject to the NDB Scheme.

To determine whether the NDB Scheme applies to your business, follow the checklist below.

Q1. Does your business handle personal information?

Personal information is information or an opinion about an identified person or a person who could reasonably be identified from the information. Even if the information you handle is anonymous or you use pseudonyms, you may still handle personal information if the information could be combined with other publicly available information to identify the person.

- **Yes** Proceed to Question 2.
- **No** The NDB scheme does not apply to you.

Q2. Have you had an annual turnover of more than $3,000,000 in any financial year since 2002?

This includes all income from all sources, but does not include assets held, capital gains or proceeds of capital gains.

- **Yes** The NDB Scheme applies to you in relation to all of the kinds of personal information you hold.
- **No** Go to Question 3.

Q3. Do you trade in personal information?

Trading in personal information means you provide a benefit or service in order for you to collect personal information or you disclose personal information for a benefit or service without the individual's consent and without being required or authorised by law. This benefit could be a payment of money, concession, subsidy or another service.

- **Yes** The NDB Scheme applies to you.
- **No** Go to Question 4.

Q4.

Are you a health service provider?

This includes medical practitioners, private hospitals, IVF and fertility clinics, gyms, private schools, childcare centres and disability service providers. You will be a health service provider if you provide a health service, which includes recording and managing and individual's health, diagnosing illnesses or disabilities and dispensing prescription or other medication. Note this can be broader thank you think so think about what health information about individuals (such as customers or members) that you hold.

Yes The NDB Scheme applies to you.

No **Go to Question 5.**

Q5.

Are you related to a larger body corporate covered by the Privacy Act?

If your business is under a holding company, a subsidiary, or a subsidiary of a holding company, or related to another body corporate under the Corporations Act 2001 which has obligations under the Privacy Act. Please check with the related or larger body corporate to confirm if it is covered by the Privacy Act.

Yes The NDB Scheme applies to you.

No **Go to Question 6.**

Q6.

Are you providing services under a Commonwealth contract?

If you provide services to, or on behalf of, Australian Government agencies or the Norfolk Island administration under a Commonwealth contract or subcontract, you are considered a Commonwealth contracted service provider. Please check the terms of any Commonwealth contract and confirm the extent to which you are required to comply with privacy laws, including the NDB Scheme.

Yes The NDB Scheme applies to you.

No **Go to Question 7.**

Q7.

Are you a reporting entity or authorised agent of a reporting entity under the Anti-Money Laundering and Counter-Terrorism Financing Act 2006?

If you provide services to, or on behalf of, Australian Government agencies or the Norfolk Island administration under a Commonwealth contract or subcontract, you are considered a Commonwealth contracted service provider. Please check the terms of any Commonwealth contract and confirm the extent to which you are required to comply with privacy laws, including the NDB Scheme.

Yes The NDB Scheme applies to you.

No **Go to Question 8.**

Q8.

Do you operate a residential tenancy database?

If you provide services to, or on behalf of, Australian Government agencies or the Norfolk Island administration under a Commonwealth contract or subcontract, you are considered a Commonwealth contracted service provider. Please check the terms of any Commonwealth contract and confirm the extent to which you are required to comply with privacy laws, including the NDB Scheme.

Yes The NDB Scheme applies to you.

No Go to Question 9.

Q9.

Are you a credit reporting business?

You are a credit reporting business if your business involves collecting, holding, using or disclosing personal information about individuals for the purpose of providing companies with information about the credit worthiness of an individual for a profit or reward.

Yes The NDB Scheme applies to you in relation to the information you hold about individuals' credit, including their consumer credit liability, repayment history, the type of credit sought and identifying information about the individual. Please ensure you check your answers to the other questions in this checklist to determine if you have obligations in relation to other personal information you hold as well.

No Go to Question 10.

Q10.

Are you a credit provider?

You are a credit provider if a substantial part of your business involves issuing credit cards or providing credit to individuals.

Yes The NDB Scheme applies to you in relation to the information you hold about individuals' eligibility for credit. Please ensure you check your answers to the other questions in this checklist to determine if you have obligations in relation to other personal information you hold as well.

No Go to Question 11.

Q11.

Do you hold Tax File Numbers (TFNs)?

You are a credit provider if a substantial part of your business involves issuing credit cards or providing credit to individuals.

Yes The NDB Scheme applies to you in relation to the tax file numbers you hold. Please ensure you check your answers to the other questions in this checklist to determine if you have obligations in relation to other personal information you hold as well.

No Go to Question 12.

Q12.

Are you an employee association registered or recognised under the Fair Work (Registered Organisations) Act 2009?

Yes The NDB Scheme applies to you.

No Go to Question 13.

Q13.

Do you conduct protected action ballots under Part 3-3 of the Fair Work Act 2009?

Yes The NDB Scheme applies to you.

No Go to Question 14.

Q14.

Are you a service provider required to comply with the data retention provisions in Part 5-1A of the Telecommunications (Interception and Access) Act 1979?

Yes The NDB Scheme applies to you.

No Go to Question 15.

Q15.

Have you voluntarily opted into the Privacy Act?

The NDB Scheme applies to you.

Yes The NDB Scheme applies to you in relation to the tax file numbers you hold. Please ensure you check your answers to the other questions in this checklist to determine if you have obligations in relation to other personal information you hold as well.

No The NDB Scheme does not apply to you. However, please ensure you check whether your business' website contains a privacy policy which states that you comply with the NDB Scheme or Privacy Act. Your privacy policy may represent to your customers that you will comply with the NDB Scheme or Privacy Act even though you may not need to.

What now?

If the NDB Scheme does apply to you, you are now subject to the Australian Privacy Principles in relation to some or all of the personal information you hold. The Principles can be viewed **here**. The principles cover:

1. Open and transparent management of personal information;
2. Anonymity and pseudonymity;
3. Collection of solicited personal information;
4. Dealing with unsolicited personal information;
5. Notification of the collection of personal information;
6. Use or disclosure of personal information;
7. Direct marketing;
8. Cross-border disclosure of personal information;
9. Adoption, use or disclosure of government related identifiers;
10. Quality of personal information;
11. Security of personal information;
12. Access to personal information; and
13. Correction of personal information.

You must comply with the principles

In the event that you believe you have breached the principles, you may be required to notify your clients. If you have a breach of your cyber systems, you may also be obliged to issue notifications to the OAIC and/or your affected clients. To see whether an event classifies as a notifiable data breach, see our **Guide to Data Breaches**.