Australian Government
Office of the Australian Information Commissioner

December 2017

Entities covered by the NDB scheme

Key points

- Agencies and organisations (entities) that already have obligations under the *Privacy Act 1988* (Cth) (Privacy Act) to secure personal information must comply with the Notifiable Data Breaches (NDB) scheme.
- This includes Australian Government agencies, businesses and not-for profit organisations that have an annual turnover of more than $3 million, private sector health service providers, credit reporting bodies, credit providers, entities that trade in personal information and tax file number (TFN) recipients.
- Entities that have Privacy Act security obligations in relation to particular types of information only (for example, small businesses that are required to secure tax file number information) do not need to notify about data breaches that affect other types of information outside the scope of their obligations under the Privacy Act.

APP entities

The NDB scheme applies to entities that have an obligation under APP 11 of the Privacy Act to protect the personal information they hold (s 26WE(1)(a)).[1] Collectively known as 'APP entities', these include Australian Government agencies and private sector and not-for-profit organisations with an annual turnover of more than $3 million. The definition of APP entity generally does not include small business operators, registered political parties, state or territory authorities, or a prescribed instrumentality of a state (s 6C). However, some businesses of any size are APP entities, including businesses that trade in personal information and organisations that provide a health service to, and hold health information about, individuals (see *Is my organisation a health service provider?*)

For more information about APP entities, see Chapter B of the *Australian Privacy Principle Guidelines* (APP Guidelines).[2]

[1] 'Personal information' is defined in s 6(1) of the Privacy Act to include information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether the information or opinion is true or not, and whether the information or opinion is recorded in a material form or not.

[2] Available online at https://www.oaic.gov.au/agencies-and-organisations/app-guidelines/chapter-b-key-concepts#app-entity.

Small business operators

A small business operator (SBO) is an individual (including a sole trader), body corporate, partnership, unincorporated association, or trust that has not had an annual turnover of more than $3 million in any financial year since 2001 (s 6D).

Generally, SBOs do not have obligations under the APPs unless an exception applies (s 6D(4)).

If an SBO falls into one of the following categories they are not exempt and must comply with the APPs, and therefore with the NDB scheme, in relation to all of their activities:

- entities that provide any health services
- entities related to an APP entity
- entities that trade in personal information – that is, entities that disclose personal information about individuals to anyone else for a benefit, service or advantage; or entities that provide a benefit, service or advantage to collect personal information about another individual from anyone else
- credit reporting bodies
- employee associations registered under the *Fair Work (Registered Organisations) Act 2009*, and
- entities that 'opt-in' to APP coverage under s 6EA of the Privacy Act.

If an SBO carries on any of the following activities it must comply with the APPs, and therefore must comply with the NDB scheme, but only in relation to personal information held by the entity for the purpose of, or in connection with, those activities:

- providing services to the Commonwealth under a contract
- operating a residential tenancy data base
- reporting under the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006*
- conducting a protected action ballot, and
- information retained under the mandatory data retention scheme, as per Part 5-1A of the *Telecommunications (Interception and Access) Act 1979*.

More information about how to determine whether a business or organisation is an APP entity or subject to the APPs for some of its activities is available at '*Privacy business resource 10: Does my small business need to comply with the Privacy Act?*'.[3]

Credit reporting bodies

A credit reporting body (CRB) is a business or undertaking that involves collecting, holding, using, or disclosing personal information about individuals for the purpose of providing an entity with information about the

[3] Available online at https://www.oaic.gov.au/agencies-and-organisations/business-resources/privacy-business-resource-10.

credit worthiness of an individual (s 6P). Credit reporting information is defined as credit information or CRB derived information about an individual (s 6(1)).

CRBs have obligations under the NDB scheme in relation to their handling of 'credit reporting information' (s 26WE(1)(b)), and in relation to their handling of any other personal information for which they have obligations under APP 11.

Credit providers

The NDB scheme applies to all credit providers whether or not they are APP entities. The section of the Privacy Act under which a credit provider is required to comply with the scheme will depend on what kind of information is involved in the data breach.

If it is 'credit eligibility information' (defined in s 6(1)) the NDB scheme will apply because of the security requirement in s 21S(1) in relation to that information.

If the credit provider is also an APP entity the NDB scheme applies in relation to other personal information because of the security requirement in APP 11.

The following kinds of organisations are considered credit providers for the purposes of the Privacy Act (s 6G):

- a bank
- an organisation or small business operator if a substantial part of its business is the provision of credit, such as a building society, finance company or a credit union
- a retailer that issues credit cards in connection with the sale of goods or services
- an organisation or SBO that supplies goods and services where payment is deferred for seven days or more, such as telecommunications carriers, and energy and water utilities
- certain organisations or SBOs that provide credit in connection with the hiring, leasing, or renting of goods.

An organisation or SBO that acquires the right of a credit provider in relation to the repayment of an amount of credit is also considered a credit provider, but only in relation to that particular credit (s 6K).

For more information about categories of credit-related personal information, see '*Privacy business resource 3: Credit reporting – what has changed*'.[4]

TFN recipients

The NDB scheme applies to Tax File Number (TFN) recipients[5] in relation to their handling of TFN information (s 26WE(1)(d)). A TFN recipient is any person who is in possession or control of a record that contains TFN information (s 11). TFN information is information that connects a TFN with the identity of a particular individual (s 6).

[4] Available online at https://www.oaic.gov.au/agencies-and-organisations/business-resources/privacy-business-resource-3-credit-reporting-what-has-changed.

[5] Referred to in the *Privacy Act* and *Privacy (Tax File Number) Rule 2015* (TFN Rule) as 'file number recipients'.

A TFN recipient may also be an APP entity or credit provider. In certain circumstances, entities that are not otherwise covered by the Privacy Act, such as state government bodies, may also be authorised to receive TFN information and will be considered TFN recipients.

The NDB scheme applies to TFN recipients to the extent that TFN information is involved in a data breach. If TFN information is not involved, a TFN recipient would only need to comply with the NDB scheme for breaches of other types of information if they are also a credit provider or APP entity.

More information about TFN recipients is available in '*Privacy business resource 12: The Privacy (Tax File Number) Rule 2015 and the protection of tax file number information*'.[6]

Overseas activities

Entities with an 'Australian link'

The NDB scheme generally extends to the overseas activities of an Australian Government agency (s 5B(1)). It also applies to organisations (including small businesses covered by the Act, outlined above) that have an 'Australian link' (s 5B(2)).

An organisation has an Australian link either because it is, in summary, incorporated or formed in Australia (see s 5B(1A) for more detail), or where:

- it carries on business in Australia or an external Territory, and
- it collected or held personal information in Australia or an external Australian Territory, either before or at the time of the act or practice (s 5B(3)).

Further information about entities that are taken to have an Australian link is available in Chapter B of the *APP Guidelines*.

Disclosing personal information overseas

If an APP entity discloses personal information to an overseas recipient, in line with the requirements of APP 8.1, then the APP entity is deemed to 'hold' the information for the purposes of the NDB scheme (s 26WC(1)). APP 8.1 says that an APP entity that discloses personal information to an overseas recipient is required to take reasonable steps to ensure that the overseas recipient does not breach the APPs in relation to the information. This means that if the personal information held by the overseas recipient is subject to loss, unauthorised access, or disclosure, the APP entity is still responsible for assessing whether it is an eligible data breach under the Privacy Act, and if it is, for notifying individuals at risk of serious harm and providing a statement to the Commissioner.

There are exceptions to the requirement in APP 8.1 to take reasonable steps. APP entities that disclose information overseas under an exception in APP 8.2 are not taken to 'hold' information they have disclosed overseas under s 26WC. In these circumstances, if the personal information held by the overseas recipient is subject to a data breach, the APP entity does not have obligations to notify about the breach under the NDB scheme.

[6] Available online at https://www.oaic.gov.au/agencies-and-organisations/business-resources/privacy-business-resource-12-the-privacy-tax-file-number-rule-2015-and-the-protection-of-tax-file-number-information.

More information about APP 8 is available in '*Privacy business resource 8: Sending personal information overseas*'.[7]

Disclosing credit eligibility information

If a credit provider discloses credit eligibility information about one or more individuals to a person, a body or a related body corporate that does not have an 'Australian link' (s 26WC(2)(a)),[8] the credit provider may also have obligations under the NDB scheme in respect of that information. In the event that credit eligibility information held by the person or related body corporate is subject to loss, unauthorised access, or disclosure, the credit provider is responsible for assessing whether there is an eligible data breach that needs to be notified to individuals at risk of serious harm and the Commissioner.

[7] Available online at https://www.oaic.gov.au/agencies-and-organisations/business-resources/privacy-business-resource-8.

[8] This section only applies to a disclosure of credit eligibility information by a credit provider to a related body corporate under s 21G(3)(b), to a person processing an application for credit made to the credit provider or to a person who manages credit provided by the credit provider under s 21G(3), or to a debt collector under s 21M(1) of the Privacy Act.