Notifiable Data Breaches scheme under the Commonwealth Privacy Act 1988

Obligations for Victorian public sector organisations

Background

The Privacy Amendment (Notifiable Data Breaches) Act 2017 inserted Part IIIC into the Commonwealth Privacy Act 1988 to establish the Notifiable Data Breaches scheme (NDB scheme). The NDB scheme came into force on the 22nd of February 2018 and requires entities captured by the scheme to notify the Office of the Australian Information Commissioner (OAIC) and affected individuals of any eligible data breaches.

Who needs to comply in the Victorian public sector?

The NDB scheme applies to entities that have obligations to protect the personal information they hold under the Privacy Act 1988. This includes Australian Privacy Principle (APP) entities, credit reporting bodies, credit providers and tax file number (TFN) recipients.

Many Victorian public sector (VPS) organisations are TFN recipients for the purposes of the Privacy Act 1988 because they receive TFN information for some of their functions. Such organisations may include Victorian government departments and agencies, universities and local councils. If a VPS organisation experiences an eligible data breach involving TFN information, they will need to comply with the NDB scheme.

The OAIC has published a list of lawful TFN recipients, available on their website. Organisations should refer to the list in determining whether or not the NDB scheme applies in respect of their functions.

VPS organisations may also report breaches that fall outside this scope to Commonwealth agencies, as good privacy practice. See our guidance below under the ‘Reporting breaches that fall outside the scope of the NDB scheme’ heading.

What is an eligible data breach?

Only breaches likely to result in serious harm will be considered eligible data breaches under the NDB scheme. The criteria for an eligible data breach is outlined in the Privacy Act 1988.

A data breach will be deemed an eligible data breach if each of the following apply:

1. There is unauthorised access to or unauthorised disclosure of personal information, or loss of personal information (where this is likely to result in unauthorised access or unauthorised disclosure). For VPS organisations, the personal information compromised must be TFN information to qualify as an eligible data breach under the NDB scheme.

---

1 The OAIC has published guidance on entities covered by the NDB scheme, available [here](#).
2 ‘TFN information’ is defined in s 6 of the Privacy Act 1988 to mean information that connects a TFN with the identity of an individual. A ‘TFN recipient’ is defined in s 11 of the Privacy Act 1988 as any person who is in possession or control of a record that contains TFN information.
3 Some exceptions from the notification requirement under the NDB scheme apply. VPS organisations should refer to the OAIC’s guidance, [Exceptions to notification obligations](#), for further information.
4 See new sections 26WE and 26WF of the Privacy Act 1988.
2. A reasonable person would conclude that the access or disclosure would be **likely to result in serious harm** to any of the affected individuals.

3. The entity has not been able to prevent the likely risk of serious harm occurring after **remedial action** is taken (see below).

**‘Likely to result in serious harm’**

VPS organisations should have regard to two main considerations when assessing whether a breach is likely to result in serious harm. Firstly, a breach will be considered likely to result in serious harm if the risk of serious harm is **more probable than not** (rather than possible). Secondly, VPS organisations will need to assess whether the harm caused to individuals by the breach is **serious enough to be captured by the NDB scheme**. Serious harm is not defined in the **Privacy Act 1988**, however examples may include psychological, reputation or financial harm.

**Taking remedial action**

If a VPS organisation takes timely, active steps to reduce the risk of serious harm to an affected individual after a data breach involving TFN information has occurred, the breach may not be deemed an eligible data breach. If the remedial action taken does prevent the serious harm posed to an individual, the entity may avoid the requirement to notify the OAIC or affected individuals under the NDB scheme. However, if the remedial action does not prevent the risk of serious harm to affected individuals, the obligation to notify remains.

**What should a VPS organisation do if they suspect a data breach?**

Under the NDB scheme, an assessment of a suspected eligible data breach must take place within 30 days. VPS organisations should start to conduct an assessment as soon as they become aware of a suspected data breach. Remedial action can occur at any time during an assessment. The obligation to notify will arise as soon as a VPS organisation forms the belief that an eligible data breach involving TFN information has actually occurred.

VPS organisations should refer to the OAIC’s guidance **Assessing a suspected data breach** if they become aware of a suspected eligible data breach.

**How to notify**

Where a VPS organisation believes that an eligible data breach has occurred, they will be required to notify the OAIC and affected individuals. The OAIC has produced a range of guidance materials that outline the methods entities can use to notify individuals, and what should be included in the **Notifiable Data Breach statement**. This statement must be completed by entities when notifying the OAIC and affected individuals. Notifying individuals of an eligible data breach provides them the opportunity to take steps to protect their personal information.

A failure to notify the OAIC of an eligible data breach is deemed an interference with privacy and will trigger the Australian Information Commissioner’s existing enforcement powers under the **Privacy Act 1988**. VPS organisations should refer to the OAIC’s Guide to Privacy Regulatory Action, available on the OAIC’s website, for more information on complying with the NDB scheme.

---

1. See OAIC’s guidance on **Identifying eligible data breaches**.

2. The news 26WG of the **Privacy Act 1988** contains a non-exhaustive list of relevant considerations for VPS organisations to refer to in assessing the likelihood of serious harm.
Reporting breaches that fall outside the scope of the NDB scheme

VPS organisations are strongly encouraged to report breaches that fall outside the scope of the NDB scheme to the Office of the Victorian Information Commissioner (OVIC). The Privacy and Data Protection Act 2014 (PDP Act) does not place direct obligations on VPS organisations to notify OVIC or affected individuals of data breaches, however OVIC will be able to assist organisations where a data breach has occurred. VPS organisations can refer to the Responding to Privacy Breaches guidance, available on OVIC’s website.

VPS organisations are also encouraged to notify OVIC of any eligible data breaches reported to the OAIC, given that an eligible data breach involving a VPS organisation would also likely involve a breach of the PDP Act. It may not always be possible for the OAIC to identify jurisdictional overlap in the case of a data breach, given the volume of notifications received under the NDB scheme, and as such the onus rests with VPS organisations to notify all relevant parties.

In some cases, VPS organisations may hold data that has been transferred from other jurisdictions. If an organisation suspects a data breach they should consider all relevant bodies that need to be notified. Even though the VPS does not have statutory obligations under the NDB scheme to report eligible data breaches that do not involve TFN information, it is good privacy practice to report any data breaches involving personal information (other than TFN information) to the relevant Commonwealth agency. For example, where a VPS organisation experiences a data breach involving personal information that is generated by, or jointly held with, a Commonwealth agency bound by the NDB scheme. This will allow the Commonwealth agency to assess the breach and report to the OAIC accordingly. VPS organisations are also encouraged to alert OVIC of any breaches involving Commonwealth data reported to Commonwealth agencies in these circumstances.

Data breaches that do not involve personal information or TFN information may still pose a security risk. VPS organisations are encouraged to report a suspected data breach involving other public sector data to OVIC’s Data Protection Team. Additionally, VPS organisations should get in contact with the Health Complaints Commissioner, regarding suspected or confirmed breaches involving health information.

How to prepare for the NDB scheme

VPS organisations have existing obligations under Information Privacy Principle (IPP) 4.1 to take reasonable steps to protect personal information they hold, and many organisations will also have obligations under the Victorian Protective Data Security Framework (VPDSF). VPS organisations should review current policies and procedures to ensure they account for existing IPP 4.1 and VPDSF obligations.

Some steps VPS organisations should take to prepare for the scheme include:

- Updating data breach response plans, to align with the implementation of the NDB scheme and the 30-day timeline for assessments of suspected data breaches.
- Reviewing systems containing TFN and personal information (for example, payroll systems).
- Reviewing governance arrangements in place and ensuring there is executive buy-in regarding the organisation’s responsibilities under the NDB scheme.

---

7 In the absence of specific contractual arrangements for reporting data breaches.
8 Contact details for OVIC’s Privacy and Data Protection teams can be found below.
9 Roles and responsibilities should be defined and communicated across the organisation, so all staff know their specific obligations should an eligible data breach occur.
• Applying the **Five Step Action Plan** under the VPDSF to identify and value information assets containing personal information, and manage any associated risks (including the application of relative security measures).
• Devising strategies for conducting an assessment of a suspected eligible data breach.
• Including obligations under the NDB scheme in relevant staff training materials.
• Reviewing relevant contracts with contracted service providers to ensure obligations for notification are clear in outsourcing arrangements.\(^\text{10}\)

The OAIC has published an overview of the NDB scheme, available on their website, which VPS organisations should refer to in preparing for the NDB scheme.

**Further Information**

Contact OVIC’s Privacy team on 1300 00 6842 (1300 00 OVIC) or at privacy@ovic.vic.gov.au

Contact OVIC’s Data Protection team on 1300 00 6842 (1300 00 OVIC) or at security@ovic.vic.gov.au

**Contact Us**

t: 1300 00 6842
e: enquiries@ovic.vic.gov.au
w: oovic.vic.gov.au

**Disclaimer**

The information in this document is general in nature and does not constitute legal advice.

---

\(^{10}\) It is important to note that reporting obligations for contracted service providers who would otherwise be bound by the NDB scheme (i.e. large companies with an annual turnover of more than $3 million) may change, where they are providing services to a VPS organisation under a State contract. Where a data breach occurs within the scope of the State contract, the contracted service provider may be exempt from their obligations under the NDB scheme (depending on the nature of the contract and the breach) and should report the breach to the VPS organisation who is the outsourcing party. This is due to the operation of s 7B(5) of the *Privacy Act 1988*. VPS organisations are encouraged to report breaches in outsourcing arrangements to OVIC.
Workflow: The NDB scheme for the Victorian public sector

Suspected data breach in VPS organisation

Does the breach involve TFN information?

- YES
- NO

Is the breach an eligible data breach?

- YES
- NO

Voluntary notification to OVIC Privacy Team and affected individuals where appropriate

Notify OAIC and affected individuals

Note: in some cases, an exception to the obligation to notify the OAIC or affected individuals may apply.

Does the breach involve other personal information?

- YES
- NO

Does the breach involve health information?

- NO
- YES

Voluntary notification to OVIC Data Protection Team for breaches involving other public sector data

Contact Health Complaints Commissioner