Office of the Victorian Information Commissioner

INFORMATION FOR AGENCIES

1300 00 6842 | ovic.vic.gov.au

Notifiable Data Breaches scheme under the *Privacy Act 1988*

Obligations for Victorian public sector organisations

Background

The *Privacy Amendment (Notifiable Data Breaches) Act 2017* inserts Part IIIC into the Commonwealth *Privacy Act 1988* to establish the Notifiable Data Breaches scheme (NDB scheme).

The NDB scheme comes into force on the 22nd of February 2018 and will require 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 will apply 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.[1]

The NDB scheme will apply to Victorian Public Sector (VPS) organisations to the extent that an eligible data breach involves TFN information.[2] Many VPS organisations are TFN recipients for the purposes of the *Privacy Act 1988* because they receive TFN information for some of their functions. The OAIC has published a list of lawful TFN recipients, available on their website. If a VPS organisation experiences an eligible data breach involving TFN information, they will need to comply with the NDB scheme.

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.

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*.[3] 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 NBD scheme.
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 with **remedial action** (see below).

[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] See new sections 26WE and 26WF of the *Privacy Act 1988*.

'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.**[4] *Serious harm* is not defined in the *Privacy Act 1988*, however examples may include psychological, reputation or financial harm.[5]

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.

For example, a staff member of a VPS organisation sends an email attachment to an incorrect recipient. The attachment contains the tax file number of a new employee. The VPS organisation takes steps to immediately contact the recipient, explaining that they have received the attachment in error. The recipient confirms in writing that the file has not been accessed, viewed or copied and permanently deletes the file. In this instance, the VPS organisation may determine that the remedial action taken prevents the breach from becoming an eligible data breach and therefore avoid the need to notify the OAIC and affected individual. See the OAIC's Identifying eligible data breaches guidance for more examples of remedial action taken to prevent an eligible data breach.

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.

[4] See OAIC's guidance on Identifying eligible data breaches.

[5] 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* (PDPA) does not place direct obligations on VPS organisations to notify OVIC or affected individuals of data breaches, however OVIC will be able to provide guidance to organisations where a data breach has occurred and assist them in containing and addressing a data breach. VPS organisations can refer to the Responding to Privacy Breaches guidance, available on OVIC's website.

VPS organisations are also **strongly** 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 PDPA. 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.

Where personal information, or TFN information, is not compromised in a data breach but other forms of public sector data are, VPS organisations should consider reporting the breach to OVIC or relevant public sector body,[6] having regard to the significance of the breach. Data breaches involving other public sector data may still pose a security risk and reporting a suspected breach to OVIC's Data Protection Team is also encouraged.

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]
- 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.[8]

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.

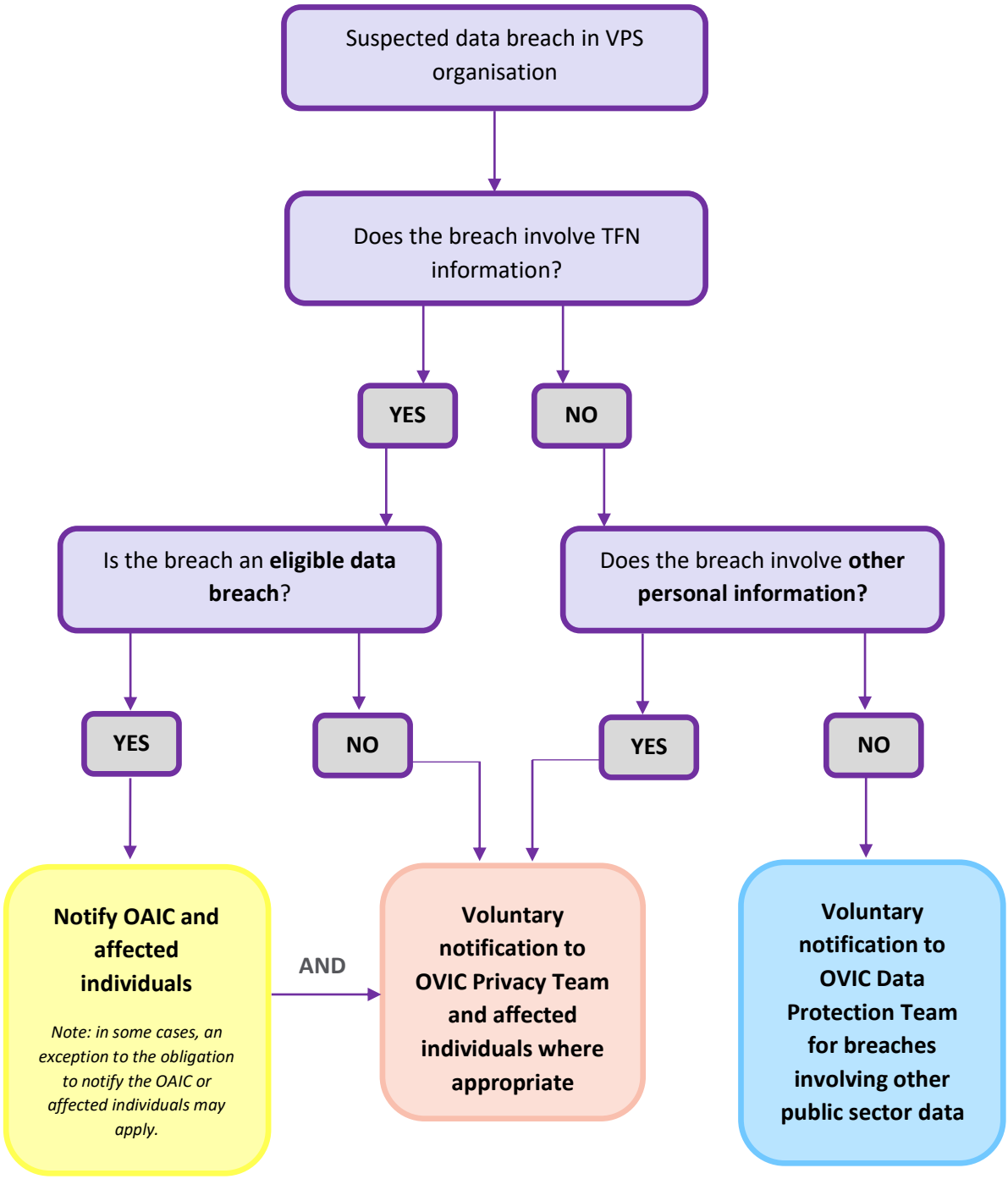
---

[6] In some cases, Victorian public sector 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 should be notified.

[7] Roles and responsibilities should be defined and communicated across the organisation, so all staff know their specific obligations should an eligible data breach occur.

[8] Note: where two or more entities hold the same personal information, only one will need to notify under the NDB scheme. In general, the entity with the most direct relationship with the affected individuals should notify both the OAIC and individuals. See the OAIC's guidance on data breaches involving more than one organisation here.

Notifiable Data Breaches scheme: When to report a data breach



Further Information

Contact Us

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

Disclaimer

Please note that the contents above are for general information purposes only, and should not be relied upon as legal advice. OVIC does not guarantee or accept legal liability whatsoever arising from, or connected to the accuracy and reliability of the contents of this information.