Global Privacy Enforcement Network 2019 Sweep

Data Breach Notifications

Every year, privacy regulators from around the world conduct a 'Sweep' to coordinate a global analysis of organisations' privacy practices.

Data breach notifications

The objective for the 2019 Global Privacy Enforcement Network (**GPEN**) Sweep was to consider how organisations handle and respond to data breaches, including how and whether data breaches are reported to privacy regulators.

During September 2019 the Office of the Victorian Information Commissioner (**OVIC**) invited 35 public sector organisations subject to the *Privacy and Data Protection Act 2014* (Vic) (**PDP Act**) to participate in the Sweep. The organisations were asked to provide a response to a questionnaire based on key aspects of successful data breach reporting and response procedures. The questions were structured under 5 indicators:

Indicator 1: Awareness of relevant data breach framework
Indicator 2: Internal procedures for handling data breaches
Indicator 3: Responding to data breaches
Indicator 4: Management
Indicator 5: Preventing future breaches

OVIC received responses from a variety of organisations, including a university, councils, government departments and statutory authorities.

OVIC submitted high-level results to the Office of the Privacy Commissioner, New Zealand (**OPCNZ**). OPCNZ was responsible for coordinating the Sweep and collating the international results.

Key findings

Some of OVIC's key findings from the Sweep include:

- **92%** of Victorian organisations were aware that OVIC encourages organisations to report data breaches to affected individuals and to OVIC even though the PDP Act did not, at the time of the Sweep, impose any mandatory breach reporting requirement upon organisations when they experience a data breach.[1]
- **33%** of Victorian organisations did not have a policy or procedure in place about reporting data breaches to the individuals affected and to OVIC. However, most of these organisations noted that if they experienced a data breach, they would consult OVIC or OVIC publications about this.
- Organisations noted many different internal thresholds for determining when to report a data breach to affected individuals or to OVIC.

[1] Under the Victorian Protective Data Security Standards v2.0 (VPDSS) Victorian public sector organisations must notify OVIC of incidents that have an adverse impact on the confidentiality, integrity or availability of public sector information with a business impact level of 2 (limited) or higher.

International results: Where does Victoria sit?

16 privacy regulators around the world examined the practices of 258 organisations. The collated international results revealed that organisations generally have a high level of knowledge about the legal framework around data breach reporting in their jurisdiction.

The international results revealed that:

- **Less than half** of organisations globally maintain up to date records of all data breaches or potential data breaches. In comparison, **all** Victorian organisations that responded maintain some records about data breaches.
- **Less than 70%** of organisations globally have a program in place to monitor internal performance in relation to their privacy obligations. In comparison, **83%** of Victorian organisations undertake monitoring of their performance in relation to their privacy obligations under the PDP Act.
- **75%** of organisations globally have a data breach response plan in place that cover key steps: containing the incident, assessing the risks of harm, notifying affected individuals and reviewing the incident to prevent future incidents of a similar nature from occurring. However, OVIC found that only **58%** of the Victorian organisations surveyed had one.

Appendix 1 contains a comparison of Victorian organisations' results to the global results against each of the 5 indicators.

Observations

OVIC was pleased to see an improvement in the percentage of Victorian organisations that have a data breach response plan, from **25%** to **75%**. This is compared to the percentage result of the Sweep conducted in 2018.

When organisations were asked how long it took them to respond to a data breach almost all said it depended on the circumstances of each incident. Only one Victorian organisation had a defined timeframe in their data breach response plan for responding to a breach.

Although all the Victorian organisations that participated in the Sweep have a dedicated individual, team, or group responsible for handling and reporting data breaches, less than half have a formal structure or process for staff across the organisation to escalate a data breach internally. As an example of good practice, one organisation has an online report form that can be accessed and completed by any staff member. Once completed, the form is sent directly to the team responsible for managing data breaches.

Recommendations

In response to the findings of the Sweep and the introduction of the Victorian Protective Data Security Standards V2.0 (**VPDSS**) in October 2019, OVIC offers the following recommendations for Victorian organisations looking to improve their data breach notification practices. OVIC suggests that organisations should:

- review data breach response plans and ensure they are in line with Victorian organisation's VPDSS obligations. Under the VPDSS, Victorian public sector organisations must notify OVIC of incidents that have an adverse impact on the confidentiality, integrity or availability of public sector information with a business impact level of 2 (limited) or higher. This obligation covers all information held by the organisation, rather than only 'personal information' as defined in section 3 of the PDP Act. To find out more refer to OVIC's Incident Notification page.
- report data breaches to affected individuals and to OVIC if there is a foreseeable risk of harm arising from the data breach.

- implement a clear structure for staff to escalate a data breach internally. This could be in the form of a guide or message on organisations' intranet page that advises staff who to contact in the event of a suspected data breach.
- check that there are timeframes included in their data breach response and escalation plans. This will help organisations act quickly in response to a data breach and gather sufficient information to notify individuals as soon as possible.
- record incidents in a data base or register and include details such as the causes of the data breach. Doing so can enable organisations to monitor trends and address causes of data breaches - for example, where an incident indicates a low level of privacy awareness or lack of processes in place to protect personal information. The data base can also help organisations monitor internal performance in relation to data protection standards.

Organisations may find it helpful to read OVIC's guide, Managing the privacy impacts of a data breach. You can also contact us, using the details below, for guidance on data breach notification.

Contact Us

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

Appendix 1 – OVIC's results

Indicator 1: Awareness of relevant data breach framework

92% of Victorian organisations were aware that personal data breach reporting to OVIC is voluntary but encouraged. **58%** of Victorian organisations correctly noted that under the Notifiable Data Breaches scheme Victorian public sector organisations must report a data breach to the Office of the Australian Information Commissioner (**OAIC**) if it involves a tax file number and the incident satisfies reporting thresholds.

In comparison, **99%** of organisations globally were aware of the legal framework in their jurisdiction.

Indicator 2: Internal procedures for handling data breaches

Internal guidance to help staff recognise a data breach

75% of Victorian organisations surveyed have internal guidance in place to assist staff to recognise a data breach. It is positive to note, however, that of the organisations without guidance in place **67%** are in the process of drafting internal guidance.

In comparison, **86%** of organisations have internal guidance in place to assist staff in recognising a breach.

Dedicated teams, groups or people within organisations to manage data breaches

All Victorian organisations surveyed have a dedicated person, group or team who breaches are reported to and managed by. OVIC cannot determine how many of these organisations have a dedicated group or team, as opposed to a person, because some of the responses were unclear.

84% of organisations globally have a dedicated team or group to manage data breaches.

Internal structure for employees to report data breaches or potential data breaches

42% of Victorian organisations reported having a structure recorded for employees to refer to when escalating incidents. Some organisations without a recorded structure noted that employees are aware of who to contact in the event of a suspected data breach, for example, because the organisation has increased staff awareness through education campaigns.

Surveyed organisations internationally outperformed Victoria in this area, as **91%** of organisations have clear policies about how data breaches should be escalated internally.

Data breach response procedure covering key steps

58% of Victorian organisations surveyed have a data breach response plan in place that cover key steps: containing the incident, assessing the risks of harm, notifying affected individuals and reviewing the incident to prevent future incidents of a similar nature from occurring.

Comparison with the international results indicates room for improvement for Victorian organisations, as **75%** of organisations globally have a data breach response procedure covering key steps.

Indicator 3: Responding to data breaches

Procedures in place to notify affected individuals about a data breach

67% of Victorian organisations said they have a procedure in place to notify affected individuals about a data breach. The amount of detail generally provided to affected individuals appears to be high, and many organisations said they would include a description of the incident, how it occurred and remedial actions taken by the organisation to minimize impact on the individuals.

Victoria performed lower in regard to notification procedures in place. **84%** of organisations globally had implemented policies or procedures around reporting breaches to individuals affected.

Procedures in place to report data breaches to OVIC

67% of Victorian organisations have a procedure in place to report data breaches to OVIC. OVIC found that a lower number of councils, compared to other types of participating organisations, had a procedure for when to report data breaches to OVIC.

In comparison, **84%** of organisations globally have a policy about when to report data breaches to the relevant privacy regulator.

Timeliness of notifying individuals or reporting data breaches to OVIC

Timeliness of reporting appears to be an issue for most of the organisations that participated in the Sweep. Very few Victorian organisations noted clear time frames, with many noting that it depends on how long it takes the organisation to investigate the incident and gather sufficient information as to when individuals are notified.

Threshold in place to determine whether to report data breaches to OVIC

OVIC received varying responses about whether organisations have a threshold for reporting breaches to OVIC. **42%** of organisations have a clear threshold in place. Of the participating organisations who did not have a clear reporting threshold in place, **86%** said they assess each incident on a case by case basis. Whilst it is positive that organisations consider the facts surrounding an incident when deciding whether to report a data breach, having a threshold in place assists organisations to maintain a consistent approach to data breach reporting.

We are unable to compare our scores with organisations globally, as this percentage result was not noted by OPCNZ in their report. Results in this area are influenced by the legal framework in each jurisdiction.

Indicator 4: Management

Maintaining records of data breaches

100% of Victorian organisations that responded indicated that they maintain records of data breaches. Organisations appeared to keep their records in different formats, from data bases that allow for tracking of trends, to folders within file management systems.

In comparison, **83%** of organisations surveyed internationally indicated they keep records on data breaches or potential data breaches.

Monitoring performance in relation to privacy obligations

83% of Victorian organisations undertake monitoring of their performance in relation to their privacy obligations under the PDP Act.

Victorian organisations performed better than average in this area. **Less than 70%** of organisations around the world monitor their performance. OPCNZ noted this as a key area of improvement for organisations across the world.

Indicator 5: Preventing future breaches

Victoria outperformed our international counterparts in regard to action taken to prevent future breaches. **100%** of organisations surveyed by OVIC said they took steps to prevent a breach in future. Steps to prevent a data breach in future generally involved a root cause analysis, increased privacy training, and a review of organisations processes to address identified risks.

This is compared to **65%** of all organisations surveyed across the world indicated that following a data breach they took steps to prevent future breaches.