

## Global Privacy Enforcement Network 2018 Sweep

### Privacy Accountability

Every year, members of the Global Privacy Enforcement Network (**GPEN**) conduct a ‘Sweep’ to coordinate a global analysis of organisations’ privacy practices. The Sweep is not an investigation or audit, nor is it intended to identify compliance issues or legislative breaches. Rather, it facilitates international collaboration and raises awareness of common global privacy issues.

For 2018, the objective of the Sweep was to consider how well organisations have implemented the concept of privacy accountability into their own internal privacy programs and policies.

### Privacy Accountability

During September 2018, the Office of the Victorian Information Commissioner (**OVIC**) contacted a random selection of 32 public sector entities that were listed on the Victorian Public Sector Commission website. These organisations were given an opportunity to self-assess their privacy practices by responding to a series of questions about privacy accountability within their organisation. Every organisation contacted for the Sweep globally was asked to respond to the same series of questions.

### Key Findings

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

- All organisations had a privacy policy or security policy, with most being publicly available.
- All organisations had a privacy officer or team, responsible for privacy governance and management. The majority of organisations have a sufficiently senior employee responsible for this.
- Most organisations did not have a dedicated incident response plan, however most had a procedure for logging incidents as they arose.
- Most organisations had an understanding of the kind of personal information they stored, however many did not have an information asset register in place. Some organisations were in the process of developing one.

### Observations

OVIC was pleased to see that all organisations had a dedicated privacy officer, privacy policy, and that privacy was generally covered as part of employee inductions.

Unfortunately, many organisations did not have an internal audit process or a dedicated incident response plan. While all organisations had some understanding of their privacy responsibilities, as demonstrated by the universal presence of a dedicated privacy officer, several organisations noted that specific business units were well versed in privacy, but those outside of those units were not. OVIC would like to see a greater focus on privacy throughout Victorian public sector organisations.

## International results: Where does Victoria sit?

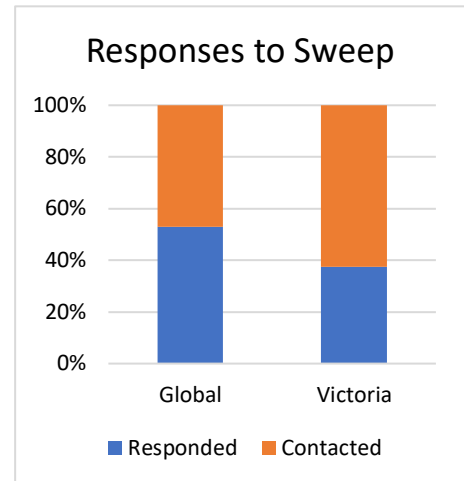
667 organisations around the world were contacted as part of the 2018 Sweep, with 53% providing substantive responses. OVIC contacted 32 organisations, with a 37.5% response rate.

A large percentage of organisations internationally had appointed an individual or team responsible for ensuring that their organisation complies with relevant privacy rules and regulations. All of the Victorian organisations that OVIC surveyed had appointed one or more of these individuals.

More than 90% of organisations had privacy policies, with most being easily accessible to the public. 100% of Victorian organisations that were surveyed had privacy policies, most of which were easily accessible.

More than 20% of organisations globally had no programs in place to conduct self-assessments or internal audits. OVIC found that 50% of responding Victorian organisations had no formal procedures for audits, however several said that they are looking to strengthen this area.

More than 50% of organisations indicated that they have formal incident response procedures. OVIC found that only 25% of responding Victorian organisations had a dedicated incident response plan.



## Recommendations

Based on the findings from the Sweep, OVIC offers the following recommendations for organisations looking to enhance their privacy accountability.

- Victorian Public Sector organisations should have a privacy policy that is publicly available and easily accessible. There should be a process in place to maintain and update this policy regularly.
- Organisations should provide refresher training for privacy, not just during employee induction.
- Organisations should look at creating formal processes for monitoring their performance in relation to privacy standards.
- Organisations should have a dedicated incident response plan in place, to identify an incident when one occurs, and respond accordingly to mitigate any risks.
- Organisations should have an information asset register in place so they are aware of the information they hold and can take appropriate steps to protect it.

---

## Further Information

### Contact Us

**t:** 1300 00 6842  
**e:** [enquiries@ovic.vic.gov.au](mailto:enquiries@ovic.vic.gov.au)  
**w:** [ovic.vic.gov.au](http://ovic.vic.gov.au)

### Disclaimer

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