OVIC
Office of the Victorian Information Commissioner
Privacy and Data Protection

Global Privacy Enforcement Network Sweep 2017

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 provide in-depth analysis or conclusively identify compliance issues or legislative breaches. Rather, it facilitates international collaboration and raises awareness of common global privacy issues. This year the objective was to examine the privacy communications and practices of a chosen sector in relation to user controls over personal information. The Sweep was conducted internationally between the 22nd – 26th May 2017.

Control over personal information in the Victorian higher education sector

The former Office of the Commissioner for Privacy and Data Protection (CPDP)[1] focused its Sweep on Victorian universities and Technical and Further Education Institutions (TAFEs), examining how they communicate their information handling practices to prospective students at the time they apply for a course. This included examining the personal information required to make a direct application to an institution, as well as considering the collection notices and general privacy policies made available to prospective students online. CPDP's intention was to consider if it was clear from a user's perspective exactly what information was collected, for what purpose, and how it would be processed, used and shared.

Key findings

Throughout the GPEN Sweep week, CPDP swept all Victorian universities that receive state funding and TAFEs that fall within the definition in the *Education and Training Reform Act 2006* – a total of 25 institutions across Victoria. Some of the key findings include:

- 32% of institutions do not adequately explain to users how their information is collected, used and disclosed.
- There was no mention of how, where and for how long personal information is stored – for example, none of the institutions swept explained whether or not personal information is kept on local servers, transferred interstate, or managed via cloud service providers.
- 88% of institutions indicated that personal information would be disclosed to third parties. However, 64% of those indicating that third party disclosure was occurring, did not give adequate detail as to who those third parties are likely to be and for what purpose the information is shared.

Observations

Overall CPDP was pleased to see that the majority of privacy communications were written in plain English, with effort being made to make them as readily understandable as possible for prospective students. However, despite policies being easy to understand, it was disappointing to see several still referring to the *Information Privacy Act 2000,* which was repealed three years ago. This indicates that privacy policies are not being regularly reviewed or updated.

Many institutions made reference to the security of the personal information they collect with a catchall comment that they 'store information securely'. CPDP would have liked to see more detail on the types of protective data security practices in place to secure students' personal information.

[1] As of the 1st of September 2017, CPDP merged with the Office of the Freedom of Information Commissioner to form the Office of the Victorian Information Commissioner.

OVIC
Office of the Victorian Information Commissioner
Privacy and Data Protection

International results: Where does Victoria sit?

Overall, 24 regulators around the world examined 455 websites and apps in sectors including retail, finance, banking, travel, social media, education and health. The collated international results revealed that website privacy notices in general are too vague and generally inadequate. This indicates that there is significant room for improvement in the quality and clarity of privacy communications around the world.

Many of CPDP's findings were reflected in the results of international counterparts. In particular, while privacy communications were generally clear on what information would be collected from a user, they fell short in relation to data security and sharing information with third parties. References to outdated legislation and frameworks is an unfortunate trend on an international scale. The Victorian higher education sector, along with many other sectors across the world, has room for improvement in how it communicates its information handling practices to its students and prospective students.

The benefits of clear communication

There are a range of benefits to communicating effectively about privacy, beyond just compliance with the law. Universities and TAFEs can create and maintain confidence with potential students by being as transparent as possible about how personal information is handled. Being clear and open about information handling practices *before* information is collected will assist individuals to make informed choices about their personal information. Further, institutions can minimise the risk of being subject to a privacy breach by making their communication on privacy matters as accessible as possible.

Tips for effective privacy communication

- Be familiar with your privacy obligations under the Information Privacy Principles (IPPs), in particular regarding privacy policies (IPP 5) and collection notices (IPP 1.3).[2] Understand that communicating clearly about privacy is beneficial to both your institution as well as prospective students.
- Where personal information is collected online, consider building collection notices into the process so they are clearly visible at the point where individuals are required to provide their personal information, rather than simply pasting a link to a privacy policy at the bottom of the page. In this context, institutions may benefit from 'layering' their collection notices. For example, by providing a concise summary on the webpage where the information is collected, and linking to more detailed notice elsewhere.
- Privacy policies should be reviewed periodically and updated where necessary to reflect changes in legislation or information management practices. Further, when an organisation adopts a new program, system or technology, it is worthwhile re-visiting privacy communications to ensure they are up to date, still comply with relevant law, and continue to reflect the flow of information.
- General privacy policies do not need to be technology-specific, however institutions may wish to include specific sections, or create stand-alone policies, to reflect their use of particular technologies or programs. Collection notices, however, should be program-specific and outline how personal information is collected, used and disclosed for particular functions.

Further details on the international findings of the 2017 GPEN Sweep are available on the Global Privacy Enforcement Network website: https://www.privacyenforcement.net/press-releases.

[2] Further guidance on drafting privacy policies and collection notices is available on the OVIC website at www.ovic.vic.gov.au.