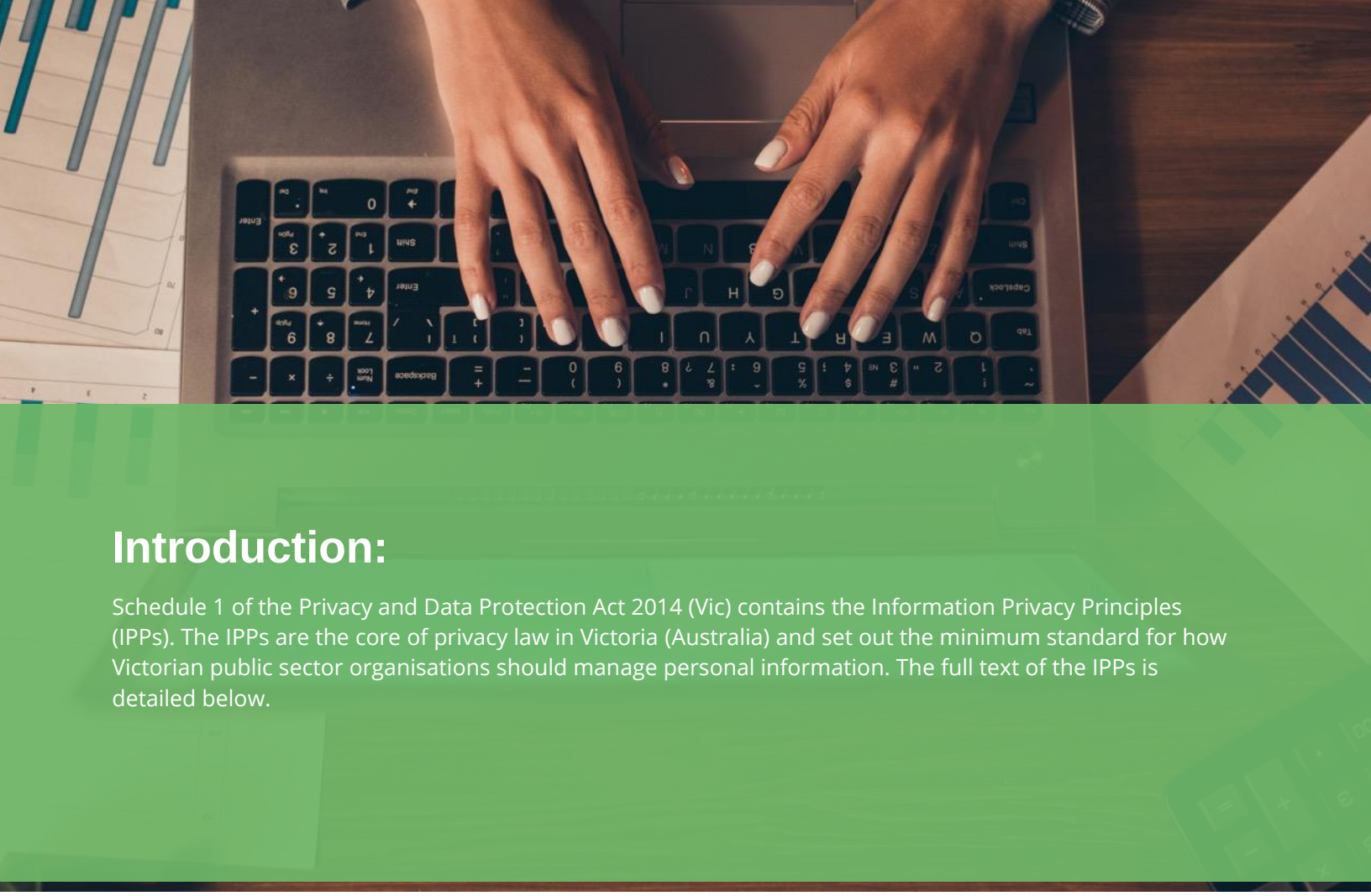
Integrity Advocate & PDP Act (2014) IPPs

Compliance Brief

Integrity Advocate



Introduction:

Schedule 1 of the Privacy and Data Protection Act 2014 (Vic) contains the Information Privacy Principles (IPPs). The IPPs are the core of privacy law in Victoria (Australia) and set out the minimum standard for how Victorian public sector organisations should manage personal information. The full text of the IPPs is detailed below.

Purpose & Scope of the IPPs

The 10 Information Privacy Principles (**IPPs**) are contained in Schedule 1 to *the Privacy and Data Protection Act 2014* (**PDP Act**) and are intended to provide high-level guidance for organizations endeavouring to achieve compliance.

Principle	Requirement	How Integrity Advocate Complies
Collection	An organisation can only collect personal information if it is necessary to fulfil one or more of its functions. It must collect information only by lawful and fair means, and not in an unreasonably intrusive way. It must provide notice of the collection, outlining matters such as the purpose of collection and how individuals can access the information. This is usually done by providing a Collection Notice, which should be consistent with an organisation's Privacy Policy.	Integrity Advocate has data minimization options that eliminate the need for ID resubmissions where the learner's image was previously validated and has developed a process that deletes all unnecessary data, including government issued ID's (where used) within 24 hours of submission.
USE AND DISCLOSURE	Personal information can only be used and disclosed for the primary purpose for which it was collected, or for a secondary purpose that would be reasonably expected. It can also be used and disclosed in other limited circumstances, such as with the individual's consent, for a law enforcement purpose, or to protect the safety of an individual or the public.	Integrity Advocate not only restricts the processing of learner information to its stated purpose of verifying identity and participation in client rules, but also acts as an intermediary and protects the redistribution of personal data where not necessary to support incidents of noncompliance.
DATA QUALITY	Organisations must keep personal information accurate, complete, and up to date. The accuracy of personal information should be verified at the time of collection, and periodically checked, as long as, it is used and disclosed by the organisation.	Integrity Advocate has an integrated process that provides all users with a copy of retained data, our review findings and reviewer notes to allow them to verify data accuracy and the conclusions drawn from the processing of their data.
OPENNESS	Organisations must have clearly expressed policies on the way they manage personal information. Individuals can ask to view an organisation's Privacy Policy.	Integrity Advocate requires informed consent from each end-user within its technology to a privacy policy that explains why their information is being requested, and how it will be used and destroyed.

DATA SECURITY	Organisations need to protect the personal information they hold from misuse, loss, unauthorised access, modification or disclosure. An organisation must take reasonable steps to destroy or permanently de-identify personal information when it is no longer needed.	Integrity Advocate encrypts user data in-transit and at rest, completes all possible data processing on the user's device (minimizing on-line traffic). To further protect user data, Integrity Advocate deletes all unnecessary data i.e., data not required to illustrate who participated in the event and/or to support any rule violations identified. The limited data retained is deleted after 24 months, unless otherwise stipulated based on a client/regulatory requirement.
ACCESS AND CORRECTION	Individuals have the right to seek access to their own personal information and to make corrections to it if necessary. An organisation may only refuse in limited circumstances that are detailed in the PDP Act. The right to access and correction under IPP 6 will apply to organisations that are not covered by the *Freedom of Information Act 1982* (Vic).	Integrity Advocate through its secure API and/or LMS integrations provides full access capabilities to authorized administrators and users to review all data retained on immediately after initial processing as well as the findings of processing.
UNIQUE IDENTIFIERS	A unique identifier is an identifier (usually a number) that is used for the purpose of identifying an individual. Use of unique identifiers is only allowed where an organisation can demonstrate that the assignment is necessary to carry out its functions efficiently. There are also restrictions on how organisations can adopt unique identifiers assigned to individuals by other organisations.	Integrity Advocate's use of unique identifiers are utilized specifically to reliably segregate data and to minimize the transmission of personally identifiable information.
ANONYMITY	Where lawful and practicable, individuals should have the option of transacting with an organisation without identifying themselves.	Anonymity is not practicable at the point of use in most situations as user identity is required for the benefit of the user. Once collected information is no longer required for it stated purpose all data is either deleted or anonymized.
TRANSBORDER DATA FLOWS	If an individual's personal information travels outside Victoria, the privacy protection should travel with it. Organisations can only transfer personal information outside Victoria in certain circumstances, for example, if the individual consents, or if the recipient of the personal information is subject to a law or binding scheme that is substantially similar to the Victorian IPPs.	Integrity Advocate's default servers are located in Canada, a jurisdiction recognized for it strong privacy laws (storage in numerous other jurisdictions is also available and is based on client preference).

SENSITIVE INFORMATION	The PDP Act places special restrictions on the collection of sensitive information. This includes racial or ethnic origin, political opinions or membership of political associations, religious or philosophical beliefs, membership of professional or trade associations or trade unions, sexual preferences or practices, and criminal record. Organisations can only collect sensitive information under certain circumstances.	No sensitive information is requested, collected, retained or transmitted as part of Integrity Advocates services.

Ref: https://ovic.vic.gov.au/privacy/resources-for-organisations/information-privacy-principles-short-guide/

Conclusion

The challenge to online services providing participation monitoring and proctoring services is to enable the best possible user experience, robust integrity controls and balance it with the required privacy protection for learners. Integrity Advocate's demonstrated compliance with the IPPs allows organizations to utilize our services with the confidence.