Integrity Advocate & PIPEDA

Compliance Brief

Integrity Advocate

Introduction:

The Personal Information Protection and Electronic Documents Act (PIPEDA) governs how the private sector collects, uses, and discloses personal information during commercial business. In addition, the Act contains various provisions to facilitate the use of electronic documents. PIPEDA became law on April 13th, 2000 to promote consumer trust in electronic commerce.

Purpose & Scope of PIPEDA

The purpose of PIPEDA is to ensure that personal information is obtained in ways that respect the fundamental right to privacy. Many organizations rely on personal information to stay in touch with their customers or clients, and to better understand how their customers are using their products and services in order to meet their needs. Ensuring that personal information is kept private is a good practice in any case, as it demonstrates respect and consideration.

In general, PIPEDA applies to organizations' commercial activities in all provinces, except Alberta, British Columbia, or Quebec, who have similar private-sector privacy laws. In the case of handling healthcare information, Ontario, New Brunswick, Newfoundland, and Labrador are also exempt due to similar legislation. In such cases, it is the substantially similar provincial law that will apply instead of PIPEDA, although PIPEDA continues to apply to interprovincial or international transfers of personal information.

Why does this matter?

The impact of PIPEDA on online educational services has been notable. These services have become more accountable for the data they possess. Their records must be organized in terms of what personal data exists, as well as documentation explaining why it has been held, who has access to it as well as other aspects of privacy management.

There is an emphasis on “Privacy by Design”; new information-handling systems and processes must be developed in accordance with regulations outlined in PIPEDA. In short, personal data must be protected from the very beginning of a product lifecycle.

Framework for Compliance

PIPEDA sets out 10 “fair information” principles that have a direct application to the online education space. These key principles include:

1. Accountability
2. Identifying Purposes
3. Consent
4. Limiting Collection
5. Limiting Use, Disclosure, and Retention
6. Accuracy
7. Safeguards
8. Openness
9. Individual Access
10. Challenging Compliance

This document explains how Integrity Advocate achieves compliance with PIPEDA as it delivers service to institutions and learners.

Principle	Requirement	How Integrity Advocate Complies
Accountability	Establish a privacy management program that complies with all 10 fair information principles; have a designated person to oversee PIPEDA compliance and the organizations' personal information protection policies and practices.	Integrity Advocate has brought its privacy management program to life by building a technology and service specifically designed to protect individual privacy. Our technology balances the need of organizations to ensure process integrity, minimize end-user support needs and to protect the privacy of participants simultaneously by: • Recognizing what is personal information, • Minimizing what we collect, • Limiting how it can be used, • Deleting what is not required as soon as it is not required, • Restricting access, and • Ensuring full transparency
Identifying Purposes	Identify and document your purposes for collecting personal information.	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
Consent	Meaningful consent is an essential element of PIPEDA. To make consent meaningful, people must understand what they are consenting to.	Integrity Advocate provides its privacy statements and policies in easy-to-understand wording and in over 60 languages to ensure end-users can provide meaningful consent.
Limiting Collection	Only collect the personal information your organization needs to fulfill a legitimate identified purpose.	Integrity Advocate limits collection by using technology in a manner that is advantageous to the privacy of end-users. Examples include monitoring if a user accesses other browser tabs and/or programs without disclosing what other programs or webpages they accessed, and not requiring users to present government-issued ID on subsequent visits when they can biometrically confirm the user against a prior confirmed image.

Limiting Use, Disclosure & Retention	Ensure the use and/or disclosure of personal information is only for the identified purposes for which it was collected. Keep only as long as it is needed, know where it is, and what is being done with it.	Unlike all other service providers of proctoring technology, Integrity Advocate does not disclose, transfer and/or give access to all the personal information collected during a session. The information shared is only the user's image and the minimum number of images required to substantiate a rule violation. Just as organizations like PayPal act as an intermediary to protect both parties in a transaction, so does Integrity Advocate. Integrity Advocate does this by providing a full review service that not only removes the administrative burden of organizations' reviewing sessions but also ensures that the private information of fully compliant users is not shared unnecessarily.
Accuracy	Minimize the possibility of using incorrect information when making a decision about an individual or when disclosing information to third parties.	Although Integrity Advocate utilizes artificial intelligence in the review of sessions it does so in a manner that requires human review and verification of all automated findings.
Safeguards	Protect personal information in a way that is appropriate to how sensitive it is.	Integrity Advocate adheres to industry standard security and quality control guidelines such as ISO 27001 (ISO/IEC 27001:2013), ISO 9001 (ISO/IEC 9001:2015), FedRAMP (NIST SP 800-53 R3) and AICPA Trust Service Criteria. We are actively seeking certifications in these standards as well as certification in the Cyber Security Alliance STAR program.
Individual Access	Advise each user of personal information your organization holds that pertains to them; Give users access to their information at minimal or no cost; Correct or amend personal information in cases where accuracy and completeness is deficient.	Integrity Advocate has eliminated the need for end-users to request access to the personal information our technology collects about them. This is done by sending an email to each individual after their session has been completed and reviewed. The email details the information retained, and the conclusions drawn.

Challenging Compliance	Provide a simple complaint-handling and investigation process. Investigate all complaints received and address all deficiencies.	As mentioned above, Integrity Advocate emails users when a session is completed. This creates complete transparency and a simple and direct method to have concerns heard and records corrected when and where required.

Conclusion

Online education services are challenged with providing a participation monitoring and proctoring service that incorporates not only the best possible user experience with robust integrity controls, but also adheres to the required privacy protection for learners. Integrity Advocate has demonstrated compliance with PIPEDA, allowing for organizations to utilize our services with confidence that **the intent of PIPEDA — as described in the 10 key principles —has been met**.

Corporate Headquarters: 13A Perron Street, Saint Albert Alberta, T8N 1N2

www.integrityadvocate.com
Customer Service Support: +1 (888) 395-1025

CSR Management: United States: +1 (650) 665-6993 | Australia: +61 2 4050 0222 | United Kingdom: +44 20 8103 9092 | Canada: +1 (226) 407-6583