

ICDL Canada
Privacy and Data Protection Legislation in Canada
Information for Candidates



Candidates entering an ICDL certification program should ensure the courseware they have selected to use properly addresses Canadian data protection legislation. Courseware included in the “Resources” section of the ICDL Canada website has been approved for use by the ECDL Foundation as well as ICDL Canada and therefore adequately covers Canadian data protection legislation. The following reference points to the section of the ICDL syllabus specific to data protection legislation:

Syllabus Version	4
Module 1	Concepts of Information Technology (IT)
Category 1.8	Copyright and the Law
Knowledge Area 1.8.2	Data Protection Legislation
Reference	1.8.2.1
Knowledge Item	Know about data protection legislation or conventions in your country. Understand the implications of data protection legislation for data subjects and data holders. Describe some of the uses of personal data.

ICDL Canada has prepared the following information about data protection legislation in Canada for both candidates and vendors to review.

Privacy and Data Protection Legislation in Canada

The **Privacy Act** and the **Personal Information Protection and Electronic Documents Act** are two federal laws ensuring that the personal information of Canadians is protected.

The **Privacy Act** took effect on July 1, 1983 and applies to federal government departments and agencies. Under the Act, Canadians have the right to access personal information held by federal government organizations. Each province has its own privacy legislation that government bodies must comply with.

The **Personal Information Protection and Electronic Documents Act (PIPEDA)** was fully implemented in Canada on January 1, 2004 and applies to all private sector organizations. The province of Quebec implemented its own private sector privacy law on November 19, 2003 and therefore is not required to comply with PIPEDA.

“Organizations covered by the Act must obtain an individual’s consent when they collect, use or disclose the individual’s personal information. The individual has a right to access personal information held by an organization and to challenge its accuracy, if need be. Personal information can only be used for the purposes for which it was collected. If an organization is going to use it for another purpose, consent must be obtained again. Individuals should also be assured that their

information will be protected by specific safeguards, including measures such as locked cabinets, computer passwords or encryption.”

“Personal information includes any factual or subjective information, recorded or not, about an identifiable individual. This includes information in any form, such as: age, name, ID numbers, income, ethnic origin, or blood type; opinions, evaluations, comments social status, or disciplinary actions; and, employee files, credit records, loan records, medical records, existence of a dispute between a consumer and a merchant and intentions (for example, to acquire goods or services, or to change jobs). Personal information does not include the name, title or business address or telephone number of an employee of an organization.” *Office of the Privacy Commissioner of Canada. Your Privacy Responsibilities. Ottawa, ON: Government of Canada, 2000.*

The following **ten principles** must be followed by all organizations regarding the collection, use and disclosure of personal information: Accountability, Identifying Purposes, Consent, Limiting Collection, Limiting Use, Disclosure and Retention, Accuracy, Safeguards, Openness, Individual Access and, Provide Recourse.

More information about Canada’s Personal Information Protection and Electronic Documents Act may be obtained from the Office of Privacy Commissioner of Canada at www.privcom.gc.ca.