

CREDANT Solutions for PIPEDA Compliance

Canadian regulation protects individual rights on personal data protection

REGULATORY OVERVIEW

The Canadian Personal Information Protection and Electronic Documents Act (PIPEDA) governs how private-sector organizations collect, use and disclose personal information in the course of commercial business—including selling, bartering or leasing of donor, membership or other fundraising lists. Enacted in April 2000, and effective January 2004, PIPEDA also governs the use of electronic documents as noted by Section 5, Principle 7 – Safeguards, specifically that “Organizations shall protect personal information regardless of the format in which it is held.”

Among its many provisions, PIPEDA provides individuals with a series of rights regarding their personal information, from understanding why an organization is using their information, to expecting their information will be kept accurate and protected, and providing individuals the right to complain about privacy violations.

THE COMPLIANCE CHALLENGE

Understanding the intricacies of PIPEDA can be confusing. PIPEDA, unlike US data protection laws, is interpreted by privacy commissioners, thus adding a layer of subjectivity. For example, encrypted data does not necessarily equal “safe harbor” but encryption is considered in determining whether unauthorized access to data could lead to future harm. And just like most regulations governing information privacy, PIPEDA contains some exceptions. For instance:

- › Information can be collected, used and disclosed without the consent of the individual for law enforcement investigations or in an emergency.
- › There are also exceptions to the general rule that an individual must be given access to his or her personal information.
- › Provinces that have “substantially similar” privacy laws are exempt from PIPEDA compliance, including:
 - An Act Respecting the Protection of Personal Information in the Private Sector (Quebec)
 - The Personal Information Protection Act (British Columbia)
 - The Personal Information Protection Act (Alberta)
 - The Personal Health Information Protection Act (Ontario)

In addition, to the exceptions it is important to note that the Commissioner may make public any information relating to the personal information management practices of an organization if they consider it is in the public interest to do so, thus adding to the criticality of selecting an experienced and proven technology solution provider.

CREDANT SOLUTION

CREDANT encryption management solutions ensure that encryption and security mandates are consistently and efficiently enforced –regardless of where the data resides.

ONLY CREDANT ENABLES ORGANIZATIONS TO:

- › Manage encryption and secure data across multiple endpoints from a common management platform
 - › Full Disk Encryption (FDE)
 - › Self-Encrypting Drives
 - › Policy-Based File/Folder Encryption
 - › Mobile Devices and Smartphones
 - › Removable Media
 - › Windows[®] BitLocker[™]
- › Create automatic audit trails that offer proof of end-to-end data security
- › Provide a transparent end-user interface that supports user productivity while keeping data safe
- › CREDANT provides you with a centrally-managed, highly scalable and architecturally flexible approach to manage all data endpoints. With CREDANT, organizations can:
 - › Help ensure data security, reducing the risk of insider or external attack
 - › Simplify and reduce the workload of maintaining compliance
 - › Provide confidentiality, privacy and auditing of data residing on any endpoint
 - › Integrate and manage multiple encryption solutions into a single management tool set