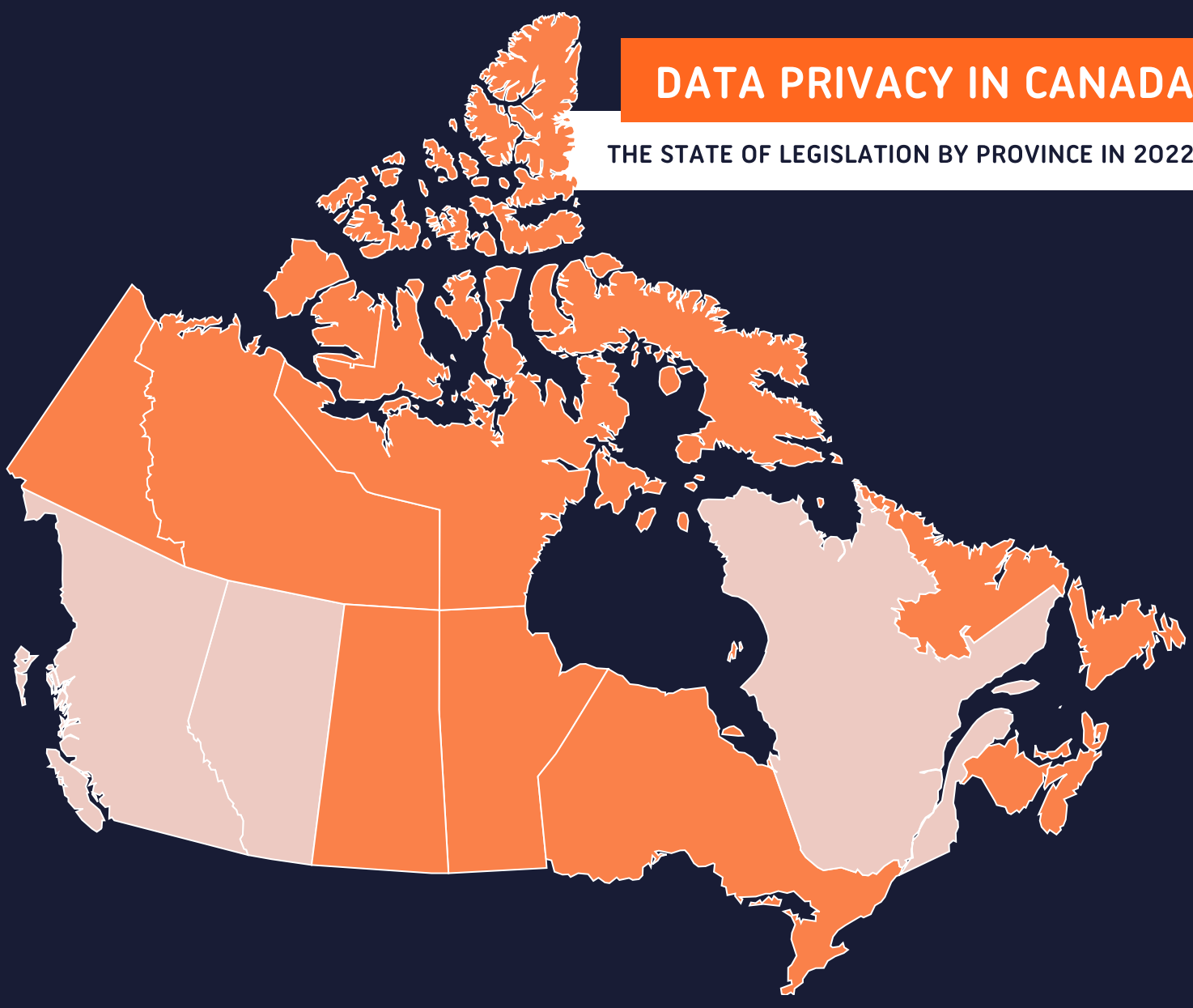
DATA PRIVACY IN CANADA

THE STATE OF LEGISLATION BY PROVINCE IN 2022



WHAT IS PIPEDA?

PIPEDA sets the ground rules for how private-sector organizations collect, use, and disclose personal information in the course of for-profit, commercial activities across Canada. It also applies to the personal information of employees of federally-regulated businesses such as: banks, airlines, and telecommunications companies.

ALTERNATE REGULATIONS

Alberta, British Columbia, and Quebec have provincial policies in place. A provincial privacy law is considered substantially similar to PIPEDA if it:

- Provides equal privacy protection
- Contains the 10 PIPEDA fair information principals
- Provides for independent oversight
- Allows the collections, use and disclosure of personal information only for legitimate purposes

These provincial policies only apply for data processing conducted 100% within that province.

10 FAIR INFORMATION PRINCIPALS OF PIPEDA

1. ACCOUNTABILITY
2. IDENTIFYING PURPOSES
3. CONSENT
4. LIMITING COLLECTION
5. LIMITING USE/DISCLOSURE/RETENTION
6. ACCURACY
7. SAFEGUARDS
8. OPENNESS
9. INDIVIDUAL ACCESS
10. CHALLENGING COMPLIANCE

PCI DSS v4.0 was officially released at the end of March 2022. As a result, organizations managing environments within its scope must prepare for significant changes to the PCI Data Security Standard (DSS) over the next 18 months.

PCI DSS V4.0

PROMOTE SECURITY AS A CONTINUOUS PROCESS

Security testing has to be a continuous process, rather than a snapshot of an organization's PCI DSS compliance taken once a year during the annual audit. Documentation tells assessors (QSAs) that they must select samples over a period of time to prove compliance.

ENHANCE VALIDATION METHODS & PROCEDURES

V4.0 contains revisions to the authentication requirements to reflect the latest industry best practices for password and multi-factor authentication (MFA). Passwords must be longer and consist of at least 12 characters containing a mixture of numbers and letters. Multi-factor authentication will become mandatory for all accounts that provide access to the card data environment.

ADD FLEXIBLITY TO ACHIEVE MORE STRINGENT SECURITY

V4.0 allows organizations to design their own controls and implement them based on the intent of the requirements in lieu of compensating controls. V4.0 supports the use of technologies, such as cloud-based hosting services, by introducing more flexible wording around requirements and adding intent statements to address the evolving threats to the payment ecosystem.

THE SOLUTION

As data privacy standards are continuously evolving, regulators encourage organizations to descope their contact centres and ensure they are free from sensitive data passing through. PCI Pal's suite of cloud-based solutions can provide this descoped process across a list of channels. Learn more here.

PCI Pal®

*Last updated April 2022, data is subject to change/evolve.
Sources: Various