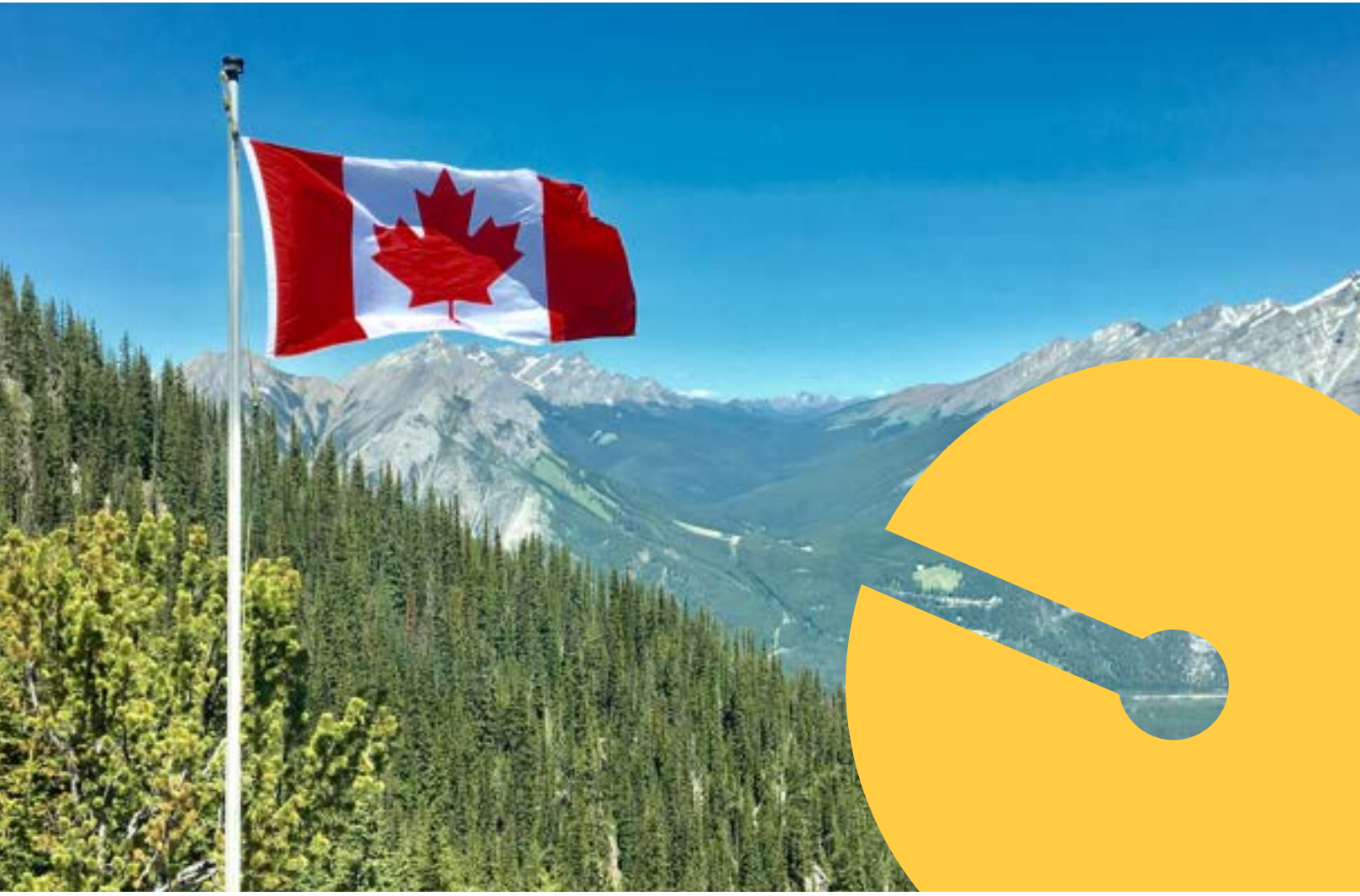
cassie

A comprehensive guide to privacy law in Canada

Guide



Introduction

What is Canada known for? Maple syrup, ice hockey, moose... How about data privacy?

As technology continues to evolve, so does the complex landscape of privacy regulations.

And just like the rest of the world, Canada is well on its way to embedding comprehensive privacy laws that safeguard personal data and build trust.

Organizations that trade within the borders of Canada need to understand and navigate Canadian privacy law carefully.

This guide aims to empower you with practical expertise and authoritative guidance, enabling you to champion a privacy-centric approach within your business (and avoid regulatory fines!).

We delve into the foundations of privacy legislation in Canada, introducing you to PIPEDA and other pertinent laws that shape data protection practices within the nation. Understanding the key concepts and terminology is essential for building a solid foundation, and we will explore the definition of personal information, consent requirements, privacy principles, and their implications for businesses.

Achieving and maintaining compliance is an ongoing commitment, demanding a proactive and multifaceted approach. Through comprehensive guidelines and actionable strategies, you will be better prepared to handle data-related challenges with confidence and precision.

Understanding the Canadian privacy law landscape

Overview of privacy laws in Canada

Canada takes data protection and privacy seriously, and businesses operating within its borders must comply with a set of robust privacy laws.

One of the primary legislations governing the collection, use, and disclosure of personal information is the Personal Information Protection and Electronic Documents Act (PIPEDA).

PIPEDA (Personal Information Protection and Electronic Documents Act)

PIPEDA is a federal privacy law that came into effect on January 1, 2004. Its primary purpose is to establish rules for the private sector's collection, use, and disclosure of personal information in the course of commercial activities. PIPEDA applies to organizations that collect, use, or disclose personal information during their business operations, except in provinces that have their own substantially similar privacy legislation.

Other relevant privacy laws and regulations in Canada (e.g., provincial laws)

In addition to PIPEDA, some provinces in Canada have their own privacy laws that apply to commercial organizations within their jurisdiction. For instance, Alberta, British Columbia, and Quebec have enacted their private-sector privacy laws that are deemed substantially similar to PIPEDA. It is essential for businesses to understand how these provincial laws align with or differ from PIPEDA to ensure full compliance with all applicable regulations.

CPPA (Canada Consumer Privacy Protection Act)

The Canada Consumer Privacy Protection Act (CPPA) is a proposed federal privacy law that is intended to replace the existing PIPEDA. The CPPA was introduced as Bill C-11 by the Canadian government in November 2020 as part of its efforts to modernize and strengthen the country's privacy laws.

The CPPA aims to enhance data privacy and protection for Canadian consumers by addressing the challenges posed by the rapid advancement of technology and the digital economy. The proposed act introduces several key changes and enhancements to the current privacy framework to provide individuals with greater control over their personal information and to increase accountability for organizations handling this data.

It is essential to note that the CPPA was introduced as a bill and may undergo further amendments and legislative processes before becoming law. The proposed act reflects the Canadian government's efforts to modernize privacy legislation to better protect individuals' personal information in the digital age. As the legislative process progresses, further updates and refinements to the CPPA may occur.

Key features of CPPA

Enhanced consent requirements

The CPPA introduces more stringent consent requirements, emphasizing explicit and informed consent for the collection, use, and disclosure of personal information.

Individual rights

The proposed act grants individuals new rights, including the right to data portability (to request their personal data in a usable format) and the right to erasure (to request the deletion of their personal information in certain circumstances).

Increased enforcement and fines

The CPPA introduces higher fines for non-compliance, with penalties reaching up to 5% of global revenue or CAD $25 million, whichever is higher, for serious violations.

Key concepts and terminology

To navigate the Canadian privacy landscape effectively, it's crucial to grasp key concepts and terminology used in privacy laws. There are some fundamental aspects that will form the foundation for your organization's compliance strategy.

Definition of 'Personal Information' under PIPEDA

PIPEDA defines personal information as any information about an identifiable individual. This includes but is not limited to names, addresses, phone numbers, email addresses, social insurance numbers, financial information, and health records. Understanding what constitutes personal information is vital as it guides the scope of your privacy protection obligations.

Consent requirements and exceptions

Consent is a fundamental principle in privacy law. PIPEDA mandates that organizations must obtain the informed consent of individuals before collecting, using, or disclosing their personal information. Consent should be obtained for specific purposes and be given voluntarily by the individual.

However, there are exceptions to the consent requirement in certain situations, such as when the collection is for legal or security reasons or when required by law enforcement. Understanding these exceptions is essential to ensure your organization's actions remain compliant with the law.

Privacy principles and their implications for businesses

PIPEDA is built on ten privacy principles that organizations must adhere to. These principles include accountability, identifying purposes for data collection, obtaining consent, limiting data collection, ensuring data accuracy, safeguarding information, and providing individuals with access to their personal data.

Canadian compliance requirements and best practices

Data collection and processing

Lawful purposes for data collection

Under Canada's data privacy laws, businesses must have a legitimate and lawful purpose for collecting personal information from individuals. This means that data collection should be directly related to the services or products the organization provides, and individuals should be made aware of the specific purposes for which their data is being collected.

Storage and retention policies

Organizations are required to establish proper data storage and retention policies to ensure that personal information is retained only for as long as necessary to fulfill the identified purposes. Implementing data retention schedules and securely disposing of data when it is no longer needed is crucial to maintaining compliance and safeguarding individuals' privacy.

Cross-border data transfers and international implications

When personal information is transferred across borders, businesses must ensure that adequate protection is maintained throughout the process. For international data transfers, organizations should take necessary measures to comply with data protection laws in both the originating and receiving countries. This may involve obtaining explicit consent from individuals or using approved data transfer mechanisms, such as Standard Contractual Clauses or Binding Corporate Rules.

Consent management

Obtaining valid consent

Consent is a cornerstone of data privacy laws in Canada. Businesses must obtain valid and informed consent from individuals before collecting, using, or disclosing their personal information. Consent should be sought in clear and plain language, providing individuals with a clear understanding of the purposes for data collection and any potential third-party disclosures. Organizations should also inform individuals of their right to withdraw consent at any time.

Consent withdrawal and updates

Data subjects have the right to withdraw their consent for the collection, use, or disclosure of their personal information. Businesses should establish simple and accessible procedures to allow individuals to withdraw their consent easily. Additionally, if the purpose of data collection changes, organizations must seek renewed consent from individuals to ensure compliance with the law.

Consent documentation and record-keeping

Maintaining accurate records of consent is crucial for demonstrating compliance with privacy laws. Organizations should document the details of consent obtained, including the date, time, and method of obtaining consent. Having a systematic approach to record-keeping helps organizations respond to any potential complaints or inquiries from regulatory authorities.

Individual rights and requests

Rights of data subjects under PIPEDA

PIPEDA grants individuals several rights regarding their personal information. These include the right to access their data, request corrections to inaccurate information, and inquire about how their data is being used and disclosed. Organizations must be prepared to address these rights promptly and provide individuals with the information they are entitled to.

Handling access requests and rectification requests

When individuals request access to their personal data, organizations should respond in a timely manner, providing the requested information in a clear and understandable format. Similarly, if individuals identify inaccuracies in their data, organizations must correct or update the information promptly and notify any third parties with whom the data was shared.

Managing data deletion and erasure requests

Data subjects have the right to request the deletion or erasure of their personal information in certain circumstances. Businesses must have processes in place to handle such requests, ensuring that data is securely and permanently deleted from all systems, except in cases where retention is legally required or justified.

Data security and breach notification

Implementing robust data security measures

Ensuring the security of personal information is of utmost importance to protect individuals' privacy. Organizations should implement robust data security measures, including encryption, access controls, firewalls, and regular security audits, to safeguard personal data from unauthorized access, disclosure, or alteration.

Preparing for and responding to data breaches

Despite robust security measures, data breaches may still occur. It is essential for organizations to have a comprehensive data breach response plan in place. This plan should include procedures for identifying and containing breaches, notifying affected individuals, and cooperating with regulatory authorities in breach investigations.

Obligations for breach notification under PIPEDA

Under PIPEDA, organizations must report certain data breaches to the Office of the Privacy Commissioner of Canada and affected individuals. The breach notification should be made as soon as feasible and should include details about the nature of the breach, the personal information involved, and the steps being taken to mitigate the impact.

Best practices for successful compliance

Proactive data security measures

Implementing robust data security measures is not only a compliance requirement but also a proactive way to safeguard sensitive information. Regular security audits, encryption, and employee training on data protection contribute to a strong security posture.

Privacy by design

Organizations that prioritize privacy from the inception of their products and services, incorporating privacy principles into the design, often face fewer compliance challenges. By embedding privacy as a core value, these companies create a culture of data protection.

Collaboration with regulatory authorities

Organizations that maintain open communication and collaboration with regulatory authorities tend to navigate privacy laws more effectively. Proactively seeking guidance and insights from privacy regulators can lead to better compliance outcomes.

Compliance challenges specific to certain industries

Different industries may face unique privacy challenges due to the nature of their data processing activities. Conduct privacy impact assessments (PIAs) to identify potential risks and implement tailored compliance measures.

Businesses in the financial services industry should adhere to PIPEDA and specific sectoral privacy laws, such as the Personal Information Protection and Electronic Documents Act for the banking sector (PIPEDA-Banking) and the Personal Information Protection and Electronic Documents Act for the insurance sector (PIPEDA-Insurance).

If your organization operates in the healthcare sector, be aware of additional privacy regulations under provincial health privacy laws. Comply with federal and provincial laws simultaneously, ensuring the protection of sensitive health information.

The role of technology in ensuring compliance

Advancements in technology have significantly transformed how businesses manage and protect data in the age of data privacy and security concerns.

Leveraging technology is now essential for organizations to ensure compliance with Canada's data privacy laws effectively.

Data mapping and inventory

Technology plays a crucial role in data mapping and inventory, enabling organizations to identify and categorize the personal data they collect and process. Data mapping tools provide an overview of data flows, helping businesses understand how information moves through their systems. This knowledge is instrumental in conducting privacy impact assessments, ensuring data accuracy, and determining compliance gaps.

Consent management platforms

Consent management platforms (CMPs) streamline the process of obtaining, managing, and tracking consent from individuals. These tools help organizations obtain explicit and granular consent, record consent preferences, and facilitate consent withdrawal when required. Advanced consent management platforms can integrate with various systems, providing a centralized and efficient approach to consent compliance.

Privacy management software

Privacy management software consolidates various compliance tasks, including policy development, risk assessments, and incident response. These platforms offer comprehensive privacy frameworks and assist organizations in designing and implementing privacy programs that align with regulatory requirements. They also help in tracking privacy-related activities, generating reports for audits, and maintaining an organized record of compliance efforts.

Achieve compliance with Cassie

Meet PIPEDA compliance requirements with Cassie: a powerful consent and preference management platform that manages over 1.2 billion customer records for large organizations handling high-volume, complex data worldwide.

Cassie's data-driven architecture integrates with third-party applications and consolidates the consents obtained using these disparate systems in a single, auditable version in compliance with codes of conduct and privacy laws.

Key platform features of Cassie:

Consent Management Platform

Manage all high-volume, complex data consents across all devices and environments

Global Privacy Compliance

Compliance with any regulation, in any language, with new legislation added as soon as it's enacted.

Preference Centre

End users can manage their own consent preferences, building trust and stronger relationships

Cookie Management module

Store consents in a centralized repository, encourage opt-ins and decrease opt-outs via user-friendly widgets across devices

Identity Service & Matching

Cassie can provide unique end user identification across states and devices using multiple identifiers and processes to match, group and assign personas

350+ API integrations

Cassie has secure, pre-built integrations across business tech stacks like CRM systems, CMS, analytics and BI platforms to form one centralized source of truth

Compliance without compromise

If you'd like to learn more about how we can help you on your compliance journey, our team of dedicated consent and preference management experts will be able to guide you every step of the way.

UK Office

0800 368 7842
+44 20 4551 9501

US Office

+1 844 585 6264

Australia Office

+61 2 5119 5048

info@trustcassie.com

trustcassie.com/contact

cassie