Comparing privacy laws: GDPR v. PIPEDA

AUGUST 2021
About the authors

OneTrust DataGuidance™ provides a suite of privacy solutions designed to help organisations monitor regulatory developments, mitigate risk, and achieve global compliance.

OneTrust DataGuidance™ regulatory research includes focused guidance around core topics (i.e. GDPR, data transfers, breach notification, among others), Comparisons which allow you to compare regulations across multiple jurisdictions at a glance, a daily customised news service, and expert analysis. These tools, along with our in-house analyst service to help with your specific research questions, provide a cost-effective and efficient solution to design and support your privacy program.

Edwards, Kenny & Bray LLP is a full-service law firm dedicated to providing business leaders with legal services that are both practical and creative. Based in Vancouver, British Columbia, EKB provides exceptional legal service in many areas, including business law, business litigation, commercial lending and finance, commercial real estate, employment, estate planning and litigation, information and privacy, mergers and acquisitions, regulatory and administrative law, and securities.

When clients engage our firm, they can expect exceptional service from lawyers recognised as exemplars in their areas of practice by publications such as Best Lawyers, Who’s Who Legal Canada, Martindale-Hubbell, and Lexpert. We’ve built our firm and our reputation on making the law work for our clients.

Contributors

OneTrust DataGuidance™: Iana Gaytandjieva, Alexander Fetani, Edidiong Udoh, Troy Boatman, Victoria Ashcroft, Matteo Quartieri

Edwards, Kenny & Bray LLP: Peter Brown, Lauren Frederick
Table of contents

Introduction

1. Scope
   1.1. Personal scope
   1.2. Territorial scope
   1.3. Material scope

2. Key definitions
   2.1. Personal data
   2.2. Pseudonymisation
   2.3. Controller and processors
   2.4. Children
   2.5. Research

3. Legal basis

4. Controller and processor obligations
   4.1. Data transfers
   4.2. Data processing records
   4.3. Data protection impact assessment
   4.4. Data protection officer appointment
   4.5. Data security and data breaches
   4.6. Accountability

5. Individuals’ rights
   5.1. Right to erasure
   5.2. Right to be informed
   5.3. Right to object
   5.4. Right to access
   5.5. Right not to be subject to discrimination in the exercise of rights
   5.6. Right to data portability

6. Enforcement
   6.1. Monetary penalties
   6.2. Supervisory authority
   6.3. Civil remedies for individuals
Introduction

On 25 May 2018, the General Data Protection Regulation (Regulation (EU) 2016/679) (‘GDPR’) went into effect. The Personal Information Protection and Electronic Documents Act (‘PIPEDA’), which regulates privacy in Canada at a federal level, was introduced on 13 April 2000 and entered into force in stages, beginning on 1 January 2001. Both pieces of legislation aim to protect individuals’ privacy and personal data, and apply to businesses’ collection, use, or sharing of personal data.

The GDPR and PIPEDA are aligned in numerous respects. Both pieces of legislation establish accountability as a fundamental legislative principle and impose similar obligations regarding territorial and material scope, implementation of security measures, and breach notification requirements. In addition, the GDPR’s definition of ‘personal data’ is similar to PIPEDA’s definition of ‘personal information’. The supervisory authority powers and responsibilities established under the GDPR and PIPEDA are, likewise, relatively aligned.

There are, however, notable differences between the GDPR and PIPEDA. Unlike the GDPR, PIPEDA only applies to organizations engaged in ‘commercial activities’ and does not apply to public bodies. Moreover, whereas the GDPR provides a list of specific legal bases for the processing of personal data, PIPEDA contains an overarching requirement that organizations may only collect, use or disclose personal information for purposes that a reasonable person would consider appropriate. In addition, whereas PIPEDA places the onus of ensuring comparable protection on organizations carrying out data transfers, the GDPR places that onus on both the exporter and recipient organizations. Other areas of differentiation include the regulation of data subjects’ rights to object to the processing of their data and to access their data.

Finally, the GDPR and PIPEDA deviate markedly in respect of several matters. For example, the GDPR expressly requires data processors to carry out a Data Privacy Impact Assessment (‘DPIA’) in certain circumstances, while PIPEDA allows organizations to carry out a Privacy Impact Assessment (‘PIA’) without establishing a requirement to do so. The GDPR and PIPEDA are also inconsistent with respect to the right to erasure, the right to be informed, and the right to data portability.

On 17 November 2020, Bill C-11 for the Digital Charter Implementation Act, 2020 (‘DCIA’) was introduced to the House of Commons. The DCIA, if enacted in a substantially similar form, would reform Canada’s federal private sector privacy laws by enacting the Consumer Privacy Protection Act and the Personal Information and Data Protection Tribunal Act. To become law, the DCIA must pass through both Houses of Parliament for consideration and receive royal assent.

This Guide highlights the similarities and differences between the GDPR and PIPEDA in order to assist organizations’ compliance with both. In addition, the Guide refers to non-binding guidance from the Office of the Privacy Commissioner of Canada (‘OPC’) which aims to clarify the OPC’s position on a range of topics. As a whole, the GDPR and PIPEDA lie between a balance of fairly consistent and fairly inconsistent in their regulation of individuals’ privacy and the protection of personal data. At the time of publication, it is unclear if or when the DCIA will receive royal assent. Therefore, this Guide does not discuss the potential impacts of the DCIA on the federal privacy regime.
Structure and overview of the Guide

This Guide provides a comparison of the GDPR and PIPEDA on the following topics:

1. Scope
2. Key definitions
3. Legal basis
4. Controller and processor obligations
5. Individuals' rights
6. Enforcement

Each topic includes relevant provisions from the GDPR and PIPEDA, an analysis of the similarities and differences between the legislative frameworks, and a summary of the comparison.

Key for giving the consistency rate

- **Consistent**: The GDPR and PIPEDA bear a high degree of similarity in the rationale, core, scope, and the application of the provision considered.

- **Fairly consistent**: The GDPR and PIPEDA bear a high degree of similarity in the rationale, core, and the scope of the provision considered, however, the details governing its application differ.

- **Fairly inconsistent**: The GDPR and PIPEDA bear several differences with regard to the scope and application of the provision considered, however, its rationale and core presents some similarities.

- **Inconsistent**: The GDPR and PIPEDA bear a high degree of difference with regard to the rationale, core, scope, and application of the provision considered.

Usage of the Guide

This Guide is general and educational in nature and is not intended to provide, and should not be relied on, as a source of legal advice. The information and materials provided in the Guide may not be applicable in all (or any) situations and should not be acted upon without specific legal advice based on particular circumstances.
### 1. Scope

The GDPR applies to data controllers and data processors, which may be natural or legal persons, public authorities, or agencies, as well as not for profit organizations. In contrast, PIPEDA does not distinguish between data controllers and data processors. Rather, PIPEDA applies to all organizations engaged in commercial activities. PIPEDA does not apply to public bodies.

Both pieces of legislation protect living individuals in relation to their personal data.

<table>
<thead>
<tr>
<th>The GDPR protects</th>
<th>The GDPR protects the personal information of individuals. ‘Individual’ is not defined in PIPEDA but guidance from the OPC, such as the OPC’s Questions and Answers, clarifies that ‘individual’ means a natural person. PIPEDA’s overall application to the personal information of deceased individuals is not entirely clear. However, PIPEDA does contain specific disclosure requirements with respect to the personal information of deceased individuals.</th>
</tr>
</thead>
<tbody>
<tr>
<td>to data controllers and data processors who may be public bodies</td>
<td>to organizations that conduct commercial activities or to personal information about an employee of, or an applicant for employment with, an organization that collects, uses, or discloses the personal information in connection with the operation of a federal work, undertaking, or business. The</td>
</tr>
</tbody>
</table>
The GDPR provides that it ‘should apply to natural persons, whatever their nationality or place of residence, in relation to the processing of their personal data.’

The term federal work, undertaking, or business is defined in PIPEDA and generally pertains to matters that are within the legislative authority of the federal government, such as shipping, railways, banks, telecommunications, and air transportation, among other activities. Whether an organization conducts commercial activities is not always immediately clear. For example, not-for-profit status does not automatically exclude an organization from the application of PIPEDA. Not-for-profit organizations that engage in commercial activities, such as selling, bartering, or leasing membership lists, are subject to PIPEDA.

PIPEDA does not explicitly refer to the nationality or place of residence of individuals. Instead, PIPEDA broadly states that personal information which is collected, used, or disclosed by organizations during the course of commercial activities will be subject to PIPEDA.
With regard to extraterritorial scope, the GDPR applies to data controllers and data processors that do not have a presence in the EU where processing activities take place in the EU. Similarly, PIPEDA applies to organizations outside of Canada if the relevant activities of the organization have a real and substantial connection to Canada.

PIPEDA does not apply to organizations that collect, use, and disclose personal information solely within a Canadian province that has enacted private sector privacy legislation which the federal government has deemed substantially similar to PIPEDA.

The GDPR applies to organisations that have a presence in the EU. In particular, per Article 3, the GDPR applies to entities or organisations established in the EU, notably entities that have an establishment in the EU or if processing of personal data takes place in the context of the activities of that establishment, irrespective of whether the data processing takes place in the EU or not.

In relation to extraterritorial scope, the GDPR applies to the processing activities of data controllers and data processors that do not have any presence in the EU, where processing activities are related to the offering of goods or services to individuals in the EU, or to the monitoring of the behaviour of individuals in the EU.

PIPEDA applies to organizations located outside Canada if the relevant activities of the organization have a real and substantial connection to Canada. The real and substantial connection test is applied on a case-by-case basis. The OPC has considered include, but are not limited to:

- the location in which the activity takes place;
- the location to which profits flow;
- the location of preparatory activities;
- the residency of parties involved;
- the location of a contract (if any);
- the jurisdiction where promotional efforts are primarily targeted;
- the location of the content provider;
- the location of the host server;
- the location of intermediaries (if any); and
- the location of the end user.
The GDPR is implemented within Member States through national laws and sets out specific areas where these laws may derogate from GDPR provisions. It is generally considered that the GDPR and Member State Laws are relatively clear in terms of their scope of application over a specific given activity. There is no equivalent within the EU.

PIPEDA does not apply to organizations that collect, use, or disclose personal information solely within a Canadian province that has enacted private sector privacy legislation which the federal government has deemed substantially similar to PIPEDA. To date, Alberta, British Columbia, and Quebec have enacted substantially similar privacy legislation and thus PIPEDA does not apply to organizations which collect, use, or disclose personal information solely within one of those provinces. However, PIPEDA applies to activities involving disclosure of personal information over provincial or international borders.

It is often unclear whether PIPEDA or provincial privacy legislation, or both, apply to a given activity. Many organizations may be subject to provincial privacy legislation in respect of certain aspects of their operations, and to PIPEDA in respect of other aspects. PIPEDA applies to all federally regulated businesses in Canada (such as banks, telephone companies, shipping companies, and railways), even within provinces which have enacted substantially similar privacy legislation.
1.3. Material scope

The definition of personal data under the GDPR and the definition of personal information under PIPEDA both relate to information regarding an identified or identifiable individual. The GDPR provides a list of information that is regarded as ‘sensitive’ and provides specific requirements for processing of sensitive data. PIPEDA does not distinguish personal information as sensitive or otherwise. However, PIPEDA does clarify that certain types of personal information will be considered sensitive and that organizations must exercise heightened care when collecting, using, or disclosing sensitive personal information in order to comply with the legislative requirements (see also the OPC guidance on Personal Information (‘the Personal Information Guidance’) and PIPEDA in Brief (‘the PIPEDA in Brief Guidance’)).

The GDPR applies to the ‘processing’ of personal data. The definition of ‘processing’ covers ‘any operation’ performed on personal data ‘such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.’

The GDPR defines ‘personal data’ as ‘any information that directly or indirectly relates to an identified or identifiable individual. The GDPR does not apply to the personal data of deceased persons.

PIPEDA applies to personal information that an organization collects, uses, or discloses in the course of commercial activities. It also imposes obligations in relation to safekeeping, access, retention, and destruction of personal information. PIPEDA does not, however, have a definition of ‘processing’.

PIPEDA applies to personal information that an organization collects, uses, or discloses in the course of commercial activities. It also imposes obligations in relation to safekeeping, access, retention, and destruction of personal information. PIPEDA does not, however, have a definition of ‘processing’.

Personal information means information about an identifiable individual. Information is generally considered personal information where there is a serious possibility that an individual could be identified through the use of the information, alone or in combination with other available information. PIPEDA is not clear with respect to its overall application to the personal information of deceased individuals, but does contain specific restrictions with respect to the disclosure of personal information of deceased individuals.

PIPEDA imposes heightened levels of care with respect to what constitutes sensitive personal information, but clarifies that any information can be sensitive depending on context. PIPEDA lists medical records and income records as examples of personal information which will almost always be considered sensitive. The OPC Interpretation Bulletin on Safeguards ('the Safeguard Guidance') clarifies that the following types of information constitutes sensitive personal information:

- medical information - considered highly sensitive;
- financial information - considered highly sensitive;

The GDPR also provides specific requirements for its processing.
### Similarities (cont’d)

<table>
<thead>
<tr>
<th>GDPR</th>
<th>PIPEDA</th>
</tr>
</thead>
<tbody>
<tr>
<td>The GDPR excludes from its application the processing of personal data by individuals for purely personal or household purposes. This is data processing that has 'no connection to a professional or commercial activity.'</td>
<td></td>
</tr>
<tr>
<td>The GDPR excludes from its application data processing in the context of law enforcement or national security.</td>
<td></td>
</tr>
<tr>
<td>The GDPR excludes anonymous data, which is defined as information that does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable.</td>
<td></td>
</tr>
<tr>
<td>The GDPR provides requirements for specific processing situations including processing for journalistic purposes and academic, artistic, or literary expression.</td>
<td></td>
</tr>
<tr>
<td>The GDPR applies to the processing of personal data by automated means or non-automated means if the data is part of a filing system.</td>
<td></td>
</tr>
<tr>
<td>• work performance information;</td>
<td></td>
</tr>
<tr>
<td>• social insurance numbers;</td>
<td></td>
</tr>
<tr>
<td>• live streaming of young children.</td>
<td></td>
</tr>
<tr>
<td>• personal or household purposes;</td>
<td></td>
</tr>
<tr>
<td>• commercial activities;</td>
<td></td>
</tr>
<tr>
<td>• federal undertaking, or business.</td>
<td></td>
</tr>
<tr>
<td>• law enforcement or national security.</td>
<td></td>
</tr>
<tr>
<td>• allows: investigations, enforcement of laws, and national security purposes.</td>
<td></td>
</tr>
<tr>
<td>• excludes anonymous data.</td>
<td></td>
</tr>
<tr>
<td>• anonymous information is not subject to or covered by PIPEDA.</td>
<td></td>
</tr>
<tr>
<td>• journalistic purposes and academic, artistic, or literary expression.</td>
<td></td>
</tr>
</tbody>
</table>

### Differences

- automated means or nonautomated means.
- does not.
2. Key definitions

2.1. Personal data

The definitions of personal data or personal information under the GDPR and PIPEDA respectively both relate to information regarding an identified or identifiable individual. However, while the GDPR provides a list of information regarded as ‘sensitive’ and provides requirements for the processing of such data, PIPEDA does not distinguish personal information as either sensitive or not. Instead, PIPEDA notes that any personal information may be sensitive depending on the context and that organizations, when collecting, using, or disclosing sensitive personal information, must exercise heightened care in order to comply with the legislative requirements.

<table>
<thead>
<tr>
<th>GDPR</th>
<th>PIPEDA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Articles 49</td>
<td>Sections 2(1), 4.01</td>
</tr>
<tr>
<td>Recitals 2630</td>
<td>Schedule 1, 4.3.4</td>
</tr>
</tbody>
</table>

**Similarities**

The GDPR defines **personal data** as ‘any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.’

PIPEDA defines **personal information** as ‘information about an identifiable individual.’

The OPC PIPEDA in Brief Guidance outlines that ‘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, identification 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, or intentions (for example, to acquire goods or services, or change jobs).

Furthermore, the Personal Information Guidance indicates that information will be personal information where there is a serious possibility that an individual could be identified through the use of that information, alone or in combination with other information.

The GDPR defines **special categories of personal data** as data revealing a data subject’s ‘racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health, or data concerning a natural person’s sexlife or sexual orientation.’

Although PIPEDA does not define what constitutes sensitive personal information, it provides that any personal information may be sensitive depending on the context, although some information, including medical and income records, is almost always considered sensitive.
The GDPR specifies that online identifiers may be considered as personal data, such as IP addresses, cookie identifiers, and radio frequency identification tags. The GDPR does not apply to 'anonymised' data, where the data can no longer be used to identify the data subject.

PIPEDA does not explicitly state that online identifiers may be considered personal information. However, the Personal Information Guidance clarifies that IP addresses, GPS tracking information, and radio frequency identification tags may be considered personal information. PIPEDA does not explicitly exclude anonymous information from its application; the definition of personal information means that anonymous information could not be personal information and thus anonymous information is not subject to or covered by PIPEDA.

Differences

Not applicable. Not applicable.
The GDPR provides a definition for pseudonymised data and clarifies that such data is subject to the obligations of the GDPR. PIPEDA neither provides a definition nor expressly regulates pseudonymised data.

The GDPR defines pseudonymised data as ‘the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.’

PIPEDA does not expressly define pseudonymised data nor does it outline specific provisions on the treatment of pseudonymised data for organizations.
Although PIPEDA does not provide definitions for data controllers and data processors, it does define the term organization. The GDPR and PIPEDA provide a similar set of responsibilities for data controllers, data processors, and organizations, specifically with regards to accountability, purpose limitation, and accuracy, among other things.

Data controllers must comply with the purpose limitation and accuracy principles, and rectify a data subject’s personal data if it is inaccurate or incomplete. Data controllers must implement technical and organizational security measures, and notify supervisory authorities of data breaches.

Organizations must also ensure the protection of personal information which must be protected by security safeguards appropriate to the sensitivity of the information. As accountability lies with organizations for personal information under their control, including information which has been disclosed to third parties, organizations must designate an individual or individuals who...
The GDPR stipulates that data controllers and data processors keep records of processing activities and provides an exception from this obligation for small organisations. The GDPR provides processes for data subject complaints as well as rights relating to accessing and rectifying personal data (see section 5. of this Guide).

A data controller is a natural or legal person, public authority, agency, or other body that determines the purposes and means of the processing of personal data, alone or jointly with others.

A data processor is a natural or legal person, public authority, agency, or other body which processes personal data on behalf of the controller.

The GDPR provides that data controllers or data processors must conduct DPIAs in certain circumstances.

Data controllers based outside the EU and involved in certain forms of processing, with exceptions based on the scale of processing and type of data, are obliged to designate a representative based within the EU in writing.

Are accountable for the organisation’s compliance with the principles established in PIPEDA.

Organisations must maintain by making information about their policies and practices relating to the management of personal information readily available to individuals.

Organisations must allow individuals the opportunity to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organisation’s compliance.

**Differences**

A is a natural or legal person, public authority, agency, or other body that determines the purposes and means of the processing of personal data, alone or jointly with others.

A is a natural or legal person, public authority, agency, or other body which processes personal data on behalf of the controller.

The GDPR provides that data controllers or data processors must conduct DPIAs in certain circumstances.

Data controllers based outside the EU and involved in certain forms of processing, with exceptions based on the scale of processing and type of data, are obliged to designate a representative based in writing.

by providing a definition for data controllers; however, PIPEDA does define the term ‘organisation’ which includes an association, a partnership, a person, or a trade union.

by providing a definition for data processors.

by establishing Privacy Impact Assessment (‘PIA’) requirements. However, an organisation may choose to complete a PIA as an aspect of its policies undertaken to give effect to the principles in Schedule 1. Furthermore, the OPC has issued its Guidance on Getting Accountability Right with a Privacy Management Program (‘the Accountability Guidance’) which recommends the use of a PIA by organisations before new products, services, or information systems are introduced or existing ones are significantly changed.

Organisations located outside of Canada which are subject to PIPEDA are . As discussed below, all organisations subject to PIPEDA are required to appoint a privacy officer. However, PIPEDA imposes no obligations with respect to the geographic location of the privacy officer.
Unlike the GDPR, PIPEDA does not impose obligations relating to children. However, the OPC has released Guidance on services aimed at children and youth (‘the Children Guidance’) which provides instructions on the collection, use, and disclosure of youth information.

### Similarities

The GDPR does not define ‘child’ or ‘children.’

When any information is addressed specifically to a child, controllers must take appropriate measures to provide information relating to processing in a concise, transparent, intelligible, and easily accessible form, using clear and plain language, that the child can easily understand.

The GDPR considers children as ‘vulnerable natural persons’ that merit specific protection with regard to their personal data. In particular, specific protection should be given when children’s personal data is used for marketing or collected for information society services offered directly to a child.

The Children Guidance provides organizations with tips regarding the collection, use, and disclosure of youth information, including:

- limiting, or avoiding altogether, the collection of personal information;
- being cautious of ‘inadvertent’ collection;
- having an appropriate retention schedule for inactive accounts;
- speaking to the specific services being provided to youth;
- making sure users can understand the organization’s privacy policies and practices, or know how to engage their parents/guardians;
- considering the user experience;
- making clear who is agreeing to terms and conditions;
- ensuring proper defaults considering the age of users;
- knowing what is happening on an organization’s site; and
- preventing unauthorised use of children’s information, as opposed to monitoring use and assuming third parties will comply with contractual obligations.

### Differences

The GDPR provides that data controllers are required to make reasonable efforts to verify that consent is given or authorised by a parent or guardian.

The Children Guidance states that organizations should ensure children’s parents or guardians are involved in the consent process where necessary.

PIPEDA does not specifically address information society services.

The GDPR applies to children’s data in relation to information society services.

PIPEDA requires organizations to make efforts to verify that parents or guardians have provided consent on behalf of children. However, the Children Guidance recommends that organizations ensure children’s parents or guardians are involved in the consent process where necessary.

PIPEDA specifically address information society services.
Where the processing is based on consent, the consent of a parent or guardian is required for providing information society services to a child below the age of 16. EU Member States can lower this age limit to 13.

The Children Guidance notes that in all but exceptional cases, consent for the collection, use, and disclosure of personal information of children under the age of 13, must be obtained from their parents or guardians.
Under the GDPR, the processing of sensitive data is not prohibited when necessary for research purposes and certain measures have been taken to safeguard the fundamental rights and interests of the data subjects. The GDPR provides specific rules for the processing of personal data for research purposes, including data minimisation and anonymisation. PIPEDA permits organizations to use and disclose personal information without consent where use or disclosure is for statistical or scholarly study or research purposes and certain other conditions are met.

According to the GDPR,

- Articles 5(1)(b), 9(2)(j), 14(5), 17(3), 21(6), 89
- Recitals 33, 159-161

According to PIPEDA, an organization is permitted to use or disclose personal information without the knowledge or consent of the individual if the personal information is used for statistical or scholarly study or research purposes.

According to PIPEDA, an organization is permitted to use or disclose personal information without the knowledge or consent of the individual if the personal information is used for statistical or scholarly study or research purposes.

Under the GDPR, the processing of personal data for research purposes is subject to specific rules (e.g. with regard to the purpose limitation principle, right to erasure, data minimisation and anonymisation etc.). Under PIPEDA, organizations may use or disclose personal information without knowledge or consent for research purposes if the research purposes cannot be achieved without using the personal information. In addition, the personal information must be used in a manner that maintains confidentiality and obtaining consent must be impracticable. Lastly, the organization must inform the OPC prior to the use or disclosure.

The GDPR clarifies that the processing of personal data for research purposes should be interpreted in a broad manner including for example technological development and demonstration, fundamental research, applied research and privately funded research.

Under the GDPR, where personal data is processed for research purposes, it is possible for Member States to derogate from some data subjects’ rights, including the

Under PIPEDA, organizations may explicitly permit organizations to derogate from particular rights of individuals for the fulfillment of research purposes.

Other than knowledge and consent, PIPEDA does not provide an equivalent provision on the scope of ‘research’ nor does it provide for derogations in the same manner as the GDPR.
right to access, the right to rectification, the right to object, and the right to restrict processing, insofar as such rights are likely to render impossible or seriously impair the achievement of the specific purposes, and such derogations are necessary for the fulfilment of those purposes.

The data subject has the right to object to the processing of personal data for research purposes unless such research purposes are for reasons of public interest.

Although under PIPEDA individuals are generally permitted to withdraw consent at any time, PIPEDA does not have an equivalent provision regarding an individual's right to object to the processing of personal information for research purposes.
3. Legal basis

Unlike the GDPR, PIPEDA does not provide a detailed list of legal bases for the processing of personal data. Instead, PIPEDA contains an overarching requirement that organizations may only collect, use, or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances.

PIPEDA requires consent prior to the collection, use, or disclosure of personal information, unless an exception applies. The OPC has issued non-binding guidance for obtaining meaningful consent from individuals, which suggests abiding by principles such as providing clear consent options, establishing innovative consent processes, and ensuring the provision of generally understandable information, among other things.

GDPR
Articles 5-10
Recitals 30-8

PIPEDA
Sections 5(3), 6.1, 7(1)-(3)
Schedule 1, 4.3

### Similarities

- consent
- specific information
- consent
- unless an exception
- applied
- nature, purpose, and consequences
- implied consent is generally appropriate for less sensitive personal information

### Differences

- categories of personal data is restricted unless explicit consent
- special heightened levels of care with respect to sensitive any information can be sensitive depending on the context
The GDPR states that data controllers can only process personal data when there is a legal ground for it. The legal grounds are:

- consent;
- when processing is necessary for the performance of a contract which the data subject is part of in order to take steps at the request of the data subject prior to entering into a contract;
- compliance with legal obligations to which the data controller is subject;
- to protect the vital interest of the data subject or of another natural person;
- performance carried out in the public interest or in the official authority vested in the data controller; or
- for the legitimate interest of the data controller when this does not override the fundamental rights of the data subject.

Further permissible uses are provided for the processing of special categories of personal data under Article 9.

Under PIPEDA, organizations may only collect, use, or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances.
4. Controller and processor obligations

Both the GDPR and PIPEDA regulate the transfer of data to third parties. However, whereas the GDPR specifically regulates international transfers with a mechanism for determining the ‘adequacy’ of protection, PIPEDA places the onus of ensuring that a comparable level of protection exists on the transferring organization for both domestic and international transfers.

Similarities

The GDPR allows personal data to be transferred to a third country or international organisation when certain requirements are met.

PIPEDA allows personal information to be transferred to a domestic or international third party for processing when certain requirements are met.

Differences

The GDPR allows personal data to be transferred to a third country or international organisation that has an adequate level of protection as determined by the European Commission. In the absence of a decision on adequate level of protection, a transfer is permitted when the data controller or data processor provides appropriate safeguards with effective legal remedies that ensure the data subjects’ rights as prescribed under the GDPR:

- Binding Corporate Rules (BCRs) with specific requirements (e.g. a legal basis for processing, a retention period, complaint procedures, etc.);
- Standard data protection clauses adopted by the European Commission or by a supervisory authority;
- An approved code of conduct;
- An approved certification mechanism.

PIPEDA provides a mechanism for establishing that a third-party organization has developed and maintains an adequate level of protection. Rather, under PIPEDA, transferring organizations for personal information transferred to third parties, as the information is considered to remain under the control of the transferring organization. Organizations must use contractual privacy protection clauses or other means to ensure while the information is being processed by the third party. The OPC’s Guidelines for Processing Personal Data Across Borders (the Crossborder Guidelines) has clarified that appropriate means include:

- Having appropriate policies and processes in place;
- Having trained its staff to ensure information is properly safeguarded at all times; and
- Having effective security measures in place.

The GDPR distinguishes between domestic and international transfers. One of the following legal grounds can be applied to the transfer of personal data abroad:

- Prior consent;
- When a data subject has explicitly consented to the proposed transfers.

PIPEDA does not distinguish between domestic and international transfers of information to third parties. Although there is no requirement for additional consent for crossborder transfers under PIPEDA, the Crossborder Guidelines note that organizations must provide notice to customers that:
transfer and acknowledged the possible risk of such transfer due to inadequate safeguards; when the transfer is necessary for the performance or conclusion of a contract; when the transfer is necessary for important public interest reasons; when the transfer is necessary for the establishment, exercise, or defence of a legal claim; and when the transfer is necessary to protect the vital interests of a data subject or other persons.

The grounds for a cross-border transfer includes the transfer being made from a register which, according to the EU or a Member States’ law, is intended to provide information to the public, and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down by EU or Member State law for consultation are fulfilled in the particular case.

Moreover, the Crossborder Guidelines has clarified that in situations where neither contractual clauses nor other means are effective in safeguarding personal information, consent may be required. PIPEDA does not specify grounds for cross-border transfers.
Global Regulatory Research Software

40 In-House Legal Researchers, 500 Lawyers Across 300 Jurisdictions

Monitor regulatory developments, mitigate risk, and achieve global compliance

OneTrust DataGuidance™
REGULATORY RESEARCH SOFTWARE
Build a global privacy program by comparing key legal frameworks against the GDPR

CCPA | Russia | Thailand | Brazil | Japan | China and 20+ other global laws & frameworks

Understand and compare key provisions of the GDPR with relevant data protection laws from around the globe

The GDPR Benchmarking tool provides comparison of the various pieces of legislation on the following key provisions:

- **Scope**
- **Rights**
- **Definitions and legal basis**
- **Enforcement**

• Employ topic specific guidance to develop your compliance activities

• Monitor news and access written opinion pieces on the most recent developments

Start your free trial at www.dataguidance.com
The GDPR requires data controllers and processors to maintain a record of processing activities. In contrast, PIPEDA does not impose specific record-keeping obligations for organizations’ processing activities.

**Similarities**

The GDPR must record:
- the name and contact details of the data controller;
- the purposes of the processing;
- a description of the categories of personal data; and
- a general description of the technical and organisational security measures that have been adopted.

Data controllers and data processors have an obligation to maintain a record of processing activities under their responsibility. The processing of information recorded by a data controller must be in writing or electronic form. The requirements around data processing records will not apply to organizations with less than 250 employees, unless the processing:
- is likely to result in a risk to the rights and freedoms of data subjects;
- is not occasional; or
- includes special categories of data in Article 9(1) (e.g. religious beliefs, ethnic origin, etc.) or is personal data relating to criminal convictions and offences in Article 10.

Under PIPEDA, organizations must record the purposes for which personal information is collected. In addition, organizations must make available information about their management of personal information, which includes:
- for the person accountable for the organization’s policies and procedures and to whom complaints or inquiries can be made;
- the means of gaining access to personal information held by the organization;
- a description of the type of personal information held by the organization, including a general account of its use; and
- what personal information is made available to related organizations.

**Differences**

Data controllers and data processors have an obligation to maintain a record of processing activities under their responsibility. The processing of information recorded by a data controller must be in writing or electronic form. The requirements around data processing records will not apply to organizations with less than 250 employees, unless the processing:
- is likely to result in a risk to the rights and freedoms of data subjects;
- is not occasional; or
- includes special categories of data in Article 9(1) (e.g. religious beliefs, ethnic origin, etc.) or is personal data relating to criminal convictions and offences in Article 10.

PIPEDA requires organizations to maintain a record of processing activities under their responsibility.
The obligations in relation to data processing records are also imposed on the representatives of data controllers.

The GDPR prescribes a list of information that a data controller must record with respect to international transfers of personal data, such as the identification of third countries or international organisations, and the documentation of adopted suitable safeguards.

PIPEDA does not impose obligations on representatives of organizations in respect of processing personal information.

PIPEDA does not prescribe information that an organization must record when transferring data to a third party.
The GDPR requires a DPIA to be conducted under specific circumstances. Although a PIA is not required under PIPEDA, an organization may conduct a PIA as part of its policies and practices implemented to give effect to the privacy principles listed in Schedule 1.

Similarities

Not applicable.

Differences

The GDPR provides that a DPIA must be conducted:

- when the processing may result in a high risk to the rights and freedoms of an individual;
- when a systematic and extensive evaluation of personal aspects relating to natural persons is involved, which is based on automated processing or profiling;
- there is processing on a large scale of special categories of data;
- there is systematic monitoring of a publicly accessible area on a large scale; and
- a data controller utilises new technologies to process personal data.

The GDPR also specifies the information that a DPIA must contain, requirements for prior consultation, and obligations for further reviews where circumstances change.

Organizations subject to PIPEDA are not required to conduct a PIA. However, the Accountability Guidance recommends the use of a PIA before new products, services, or information systems are introduced or existing ones are significantly changed. In addition, an organization may choose to complete a PIA as part of its policies and procedures undertaken to give effect to the Schedule 1 principles.
The GDPR requires the appointment of a DPO in specified circumstances. In contrast, PIPEDA requires all organizations to designate an individual or individuals to be accountable for ensuring the organization’s compliance with the principles set out in Schedule 1.

If a DPO is appointed, then data subjects may contact the DPO with regard to the processing of their personal data as well as the exercising of their rights. Contact details of the DPO must be included in the privacy notice for data subjects, and they must be communicated to the supervisory authority.

Under the GDPR, a DPO’s tasks include:
- informing and advising the controller or the data processor and the employees who carry out processing of their obligations pursuant to the GDPR and to other Union or Member State data protection provisions;
- monitoring compliance with the GDPR with other Union or Member State data protection provisions and with the policies of the data controller or data processor in relation to the protection of personal data, including the assignment of responsibilities, awareness raising and training of staff involved in processing operations, and the related audits; and
- acting as a contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to in Article 36, and to consult, where appropriate, with regard to any other matter.

The privacy officer(s) must act as the point of contact for individuals with compliance concerns. The name or title, and the address, of the privacy officer(s) must be made readily available.

Guidance from the OPC, including the PIPEDA Self-Assessment Tool and the Accountability Guidance, outline the responsibilities of privacy officers, which include informing and monitoring compliance, as well as acting as a point of contact, among other things.

Under PIPEDA, all organizations are required to designate an individual or individuals who are accountable for ensuring the organization’s compliance with the principles set out in Schedule 1. The Accountability Guidance refers to these individuals as privacy officers.
the core activities of a data controller or data processor consist of processing operations which, by virtue of their nature, their scope, and/or their purposes, require of data subjects on a large scale; or the core activities of the controller or the processor relate to a large scale of (e.g. religious beliefs, ethnic origin, data required for the establishment, exercise, or defence of legal claims etc.)

The GDPR recognises the of DPOs. PIPEDA explicitly recognise the independence of privacy officers.
Both the GDPR and PIPEDA require organizations to implement appropriate security measures with respect to personal information. In addition, the GDPR and PIPEDA provide lists of physical, organizational, and technological measures that organizations may utilise in the safeguarding of personal information.

Both the GDPR and PIPEDA contain mandatory data breach notification provisions. However, the GDPR provides exceptions to its data breach notification provisions, whereas PIPEDA does not.

The GDPR recognises integrity and confidentiality of protection by stating that personal data must be processed in a manner that ensures the security of the personal data.

The GDPR states that data controllers and data processors are required to implement appropriate technical and organisational security measures to ensure that the processing of personal data complies with the obligations of the GDPR.

The GDPR provides a list of technical and organisational measures, where appropriate, that data controllers and data processors may implement such as pseudonymisation, encryption, and the ability to restore availability and access to personal data in a timely manner in the event of physical or technical incidents, to ensure integrity and confidentiality.

In the case of a personal data breach, the data controller must notify the competent supervisory authority of the breach, unless the personal data breach is unlikely to result in a high risk to the individuals’ rights and freedoms.

Under the GDPR, data controllers must notify the competent supervisory authority of personal data breaches and, where feasible, 72 hours after having become aware of the breach.

The controller must the controller of a data breach without undue delay if the data breach is likely to result in a breach of security safeguards involving the individual’s personal information under the organization’s rights and freedoms of natural persons.

All organizations subject to PIPEDA are required to protect personal information against loss or theft, as well as unauthorised access, disclosure, copying, use, or modification.

The safeguards employed to protect the personal information must be appropriate to the sensitivity of the information.

PIPEDA provides a list of physical, organizational, and technological measures that organizations may utilise in the safeguarding of personal information.

In the case of a breach of personal information under its control, an organization must notify the OPC if it is reasonable in the circumstances to believe that the breach creates a real risk of significant harm to an individual.

Under PIPEDA, the OPC must be notified of the personal data breach as soon as feasible after the organization determines that the breach has occurred.

Unless otherwise prohibited by law, an organization must notify an individual of any breach of security safeguards involving the individual’s personal information under the organization’s rights and freedoms of natural persons.
The GDPR provides a list of information that must be, at minimum, included in the notification of a personal data breach. For example, a notification must describe the nature of the breach, the approximate number of data subjects concerned, and the consequences of the breach.

The GDPR states that the data controller must notify the data controller without undue delay after becoming aware of the personal data breach.

The GDPR requires data controllers to document any personal data breaches, comprising the facts relating to the personal data breach, its effects, and the remedial action taken.

Under the GDPR, the obligation of data controllers to notify data subjects when the data breach is likely to result in a high risk to the rights and freedoms of natural persons such as where:

- appropriate technical and organisational protective measures have been implemented;
- any subsequent measures have been taken in order to ensure that the risk is no longer likely to materialise; or it would involve disproportionate effort.

control if it is reasonable in the circumstances to believe that the breach creates of significant harm to the individual. The notification to the individual must be given as soon as feasible after the organisation determines that the breach has occurred.

Regulation SOR 2018-64 provides a list of information that in the notification to the OPC and affected individuals of a breach of security safeguards. For example, a notification must contain a description of the circumstances of the breach and a description of the personal information that is the subject of the breach.

When an organisation notifies an individual of a breach of security safeguards, it must also notify an of the breach if it believes that the other organisation or government institution may be able to reduce the risk of harm that could result from the breach. This notification must be given as soon as feasible after the organisation determines that the breach has occurred.

Organisations subject to PIPEDA must keep and maintain of every breach of security safeguards involving personal information under its control.

Under the GDPR, the obligation to the requirement to notify individuals when the breach of security safeguards creates a real risk of significant harm to the individual.

PIPEDA to the requirement to notify individuals when the breach of security safeguards creates a real risk of significant harm to the individual.
Both the GDPR and PIPEDA explicitly refer to the concept of accountability as a fundamental principle of the protection of information.

The GDPR recognises accountability as a fundamental principle of data protection. Article 5 states that ‘the data controller shall be responsible and able to demonstrate compliance with, paragraph 1 [accountability]’. In addition, the principles can be taken to apply to several other principles as mentioned in other sections of this report, including the appointment of a DPO, and DPIAs.

PIPEDA recognises accountability as a fundamental principle of the protection of information. Section 5(1) states that ‘every organization shall comply with the obligations set out in Schedule 1.’ The accountability principle described in Schedule 1 can be taken to apply to several sections of this Guide, including the transfer of data to third parties and the appointment of a privacy officer.
5. Individuals’ rights

The GDPR provides data subjects with the right to erasure and stipulates requirements relating to grounds for exercising the right, when fees are applicable, and the information that must be provided to data subjects regarding the right, among other things. While PIPEDA does not contain an equivalent express right, it outlines obligations for deleting or de-identifying personal information irrespective of any request from an individual, and provides that organizations must develop guidelines and implement procedures to govern the destruction of personal information.

Not applicable.

Differences

The right to erasure applies to specific grounds, such as where:
- consent of the data subject is withdrawn and there is no other legal ground for processing, or the personal data is no longer necessary for the purpose for which it was collected.

The GDPR also sets out several requirements covering the process of exercising this right, including informing data subjects, specific exceptions, how requests can be made, and timelines for responses, among others.

The GDPR also requires that the period for which personal data are stored are minimised, and that time limits should be established by data controllers for erasure or periodic review.

PIPEDA provides individuals with the right to erasure. Rather, PIPEDA states that personal information that is no longer required to fulfill the purposes for which it was collected should be destroyed, erased, or anonymised. PIPEDA requires organizations to develop guidelines and implement procedures to govern the destruction of personal information.

PIPEDA further outlines that individuals must be able to challenge compliance with PIPEDA’s principles, and organizations must put in place procedures to receive and respond to complaints.

When an individual successfully demonstrates the inaccuracy or incompleteness of personal information, the organization must amend the information as required. Amendment may involve the correction, deletion, or addition of information, and where appropriate, this amendment should be transmitted to third parties with access to the information.
The GDPR recognises the right to be informed and imposes an obligation to provide individuals with specific information relating to the ‘processing’ of personal data.

PIPEDA does not generally recognise an individual’s right to be informed in the same manner as the GDPR. Rather, consent under PIPEDA is only valid if it is reasonable to expect that an individual to whom the organization’s activities are directed would understand the nature, purpose, and consequences of the collection, use, or disclosure of the personal information to which they are consenting.

**Similarities**

- Data subjects should be informed of the purposes of processing in order to validate consent.
- Data subjects must be provided with information relating to the processing of personal data in order to validate their consent, including:
  - details of personal data to be processed;
  - data subjects’ rights (e.g. the right to erasure, right to object, right of withdrawal, right to lodge a complaint to a relevant authority, etc.);
  - purposes of processing, including the legal basis for processing;
  - recipients or their categories of personal data; and
  - contact details of the data controller or its representative and the DPO.
- The GDPR establishes several other obligations relating to the right to be informed, such as restricting processing for additional purposes, the format of information provided, informing of transfers, automated decision making, and data retention periods, as well as regulating when information should be provided.

**Differences**

- PIPEDA does not explicitly recognise an individual’s right to be informed of the collection, use, or disclosure of personal information, so long as certain conditions are met with respect to the collection, use, or disclosure of such information.
- Consent under PIPEDA, though, is only valid if it is reasonable to expect that an individual to whom the organization’s activities are directed would understand the nature, purpose, and consequences of the collection, use, or disclosure of the personal information to which they are consenting.
- In limiting the collection of personal information to that which is necessary, organizations must specify the type of information collected as part of their information-handling policies and practices.
Both the GDPR and PIPEDA provide individuals with the right to withdraw consent to the processing of personal information. Unlike PIPEDA, the GDPR provides a right to object to the processing of personal information in certain circumstances. PIPEDA instead allows individuals to challenge an organization’s compliance with the consent requirement, and organizations must develop procedures for responding to such complaints.

Data subjects will have the right to withdraw their consent to the processing of their personal data at any time. PIPEDA allows individuals to withdraw consent at any time, subject to legal or contractual restrictions and reasonable notice. Organizations must inform individuals of the implications of withdrawing consent. However, organizations are entitled to retain the data for the period in which it is necessary to fulfil the purpose for which it was collected.

Under the GDPR, data subjects are provided with the right to object to the processing of their personal data in specific circumstances:

- the processing of personal data is due to tasks carried out in the public interest or based on a legitimate interest pursued by the data controller or third party;
- the processing of personal data is for direct marketing purposes;
- the processing of personal data is for scientific or historical research, or statistical purposes.

The data subject has the right to be informed about the right to object, and must be informed of information about how to exercise that right. The GDPR also establishes procedures for responding to objection and restriction of processing requests.

Upon receiving withdrawal of an individual’s consent, the data controller must facilitate the exercise of the data subject’s rights, which will require the data controller to instruct the data processor to end processing of the information.

Upon receiving withdrawal of an individual’s consent, PIPEDA require organizations to inform individuals of their right to withdraw consent or how to exercise that right. Upon receiving withdrawal of an individual’s consent, PIPEDA require organizations to contact other organizations to which it has disclosed information to inform those organizations of the withdrawal of consent.
Both the GDPR and PIPEDA provide individuals with a right to access their personal information. The GDPR specifies that, when responding to an access request, the data controller must provide certain information. PIPEDA contains no such requirement.

### Similarities

The GDPR recognises that data subjects have the right to access their personal data that is processed by a data controller. The GDPR provides that the right of access must not adversely affect the rights or freedoms of others, including those related to trade secrets.

Data subjects’ requests under this right must be replied to without undue delay and in any event within one month from the receipt of a request. The deadline can be extended by two additional months taking into account the complexity and number of requests. In any case, the data subject must be informed of such an extension within one month from the receipt of a request. The right to access can be exercised free of charge. There may be some instances where a fee may be requested, notably when the requests are unfounded, excessive, or have a repetitive character.

An organization must respond to an individual’s access request within a reasonable time, but in any case not later than 30 days after receipt of the request unless this time limit is extended. The response to an individual’s request must be provided at a minimal or no cost to the individual.

### Differences

The GDPR specifies that, when responding to an access request, the data controller must indicate the existence of the right to request from the controller the rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing.

PIPEDA requires organizations to provide specific information upon receiving an access request. However, if an individual demonstrates that personal information about the individual held by an organization is incorrect, then the organization must correct the personal information.
The GDPR sets out information that must be provided when responding to an access request, reasons for refusing a request, the means through which requests may be made, and requirements to have mechanisms in place to identify requests from data subjects whose personal data is to be deleted.

While specific identity verification mechanisms are not mandated under PIPEDA, individuals may be required to provide sufficient information to enable the organization to offer an account of the requested personal information.
The right not to be subject to discrimination in exercising rights is not explicitly mentioned in the GDPR or PIPEDA. However, under the GDPR the right not to be subject to discrimination can be inferred from the fundamental rights of the data subject. In Canada, laws other than PIPEDA grant individuals the right not to be subject to discrimination.

<table>
<thead>
<tr>
<th>Similarities</th>
<th>Differences</th>
</tr>
</thead>
<tbody>
<tr>
<td>The GDPR does not explicitly address the right not to be subject to discrimination; therefore, no scope of implementation is defined.</td>
<td>Not applicable.</td>
</tr>
<tr>
<td>PIPEDA does not explicitly address the right not to be subject to discrimination; therefore, no scope of implementation is defined. However, other Canadian laws do address and prohibit discrimination.</td>
<td>Not applicable.</td>
</tr>
</tbody>
</table>

Bit applicable. Bit applicable.
The GDPR provides data subjects with the right to data portability, whereas PIPEDA does not contain an equivalent right.

**Similarities**

Not applicable.

**Differences**

The GDPR provides individuals with the right to data portability, and defines the right to data portability as the right to receive data processed on the basis of a contract or consent and processed by automated means, in a 'structured, commonly used, and machine-readable format' and to transmit that data to another controller without hindrance.

PIPEDA does not include a direct equivalent to the right to data portability.

The GDPR provides individuals with the right to data portability, whereas PIPEDA does not include a direct equivalent to the right to data portability.
6. Enforcement

Both the GDPR and PIPEDA impose monetary penalties for non-compliance, although amounts vary significantly. In addition, supervisory authorities have the power to issue penalties under the GDPR, while under PIPEDA, supervisory authorities refer these infringements to the judiciary.

The GDPR provides for the imposition of administrative monetary penalties for non-compliance. PIPEDA provides for the imposition of monetary penalties on organizations for committing an offence under PIPEDA.

The GDPR has only one category of administrative fine, which also applies to government bodies. Depending on the violation, the penalty may be up to either 2% of the global annual turnover or €10 million, whichever is higher; or 4% of the global annual turnover or €20 million, whichever is higher. Under the GDPR, it is left to Member States to create rules on the application of administrative fines to public authorities and bodies.

By oences punishable on summary conviction, fines do not exceed €6,610. By i, fines do not exceed €66,140. The OPC does not have the power to issue fines for non-compliance with PIPEDA. Rather, the OPC can issue findings and make recommendations which are subsequently referred to judicial courts who then determine whether to issue monetary penalties for non-compliance with PIPEDA.

PIPEDA does not elucidate factors to consider when applying administrative sanctions. PIPEDA provides that the following conduct constitutes an offence:

- obstructing the OPC in an investigation;
- failing to report security breaches involving personal information under an organization's control;
- failing to maintain records of security breaches involving personal information under an organization's control;
- disciplining a whistleblower.
where measures referred to in Article 58(2) have previously been ordered against the controller or processor concerned with regard to the same subject matter, compliance with those measures;

• adherence to approved codes of conduct or approved certification mechanisms;

• any other aggravating or mitigating factor applicable to the circumstances of the case.

Supervisory authorities may develop guidelines that establish further criteria to calculate the amount of the monetary penalty. The OPC does not administer fines and as such has not developed guidelines on the same.
Both the GDPR and PIPEDA provide supervisory authorities with investigatory powers including the power to obtain information and access premises. However, the GDPR provides supervisory authorities with significantly more corrective powers to ensure compliance, while PIPEDA directs these powers to the Federal Court.

Under the GDPR, supervisory authorities have investigatory powers which include:
- ordering a controller and processor to provide information required;
- conducting data protection audits;
- carrying out a review of certifications issued; and
- obtaining access to all personal data and to any premises.

Under PIPEDA, the OPC has investigatory powers, including the power to:
- summon and enforce the appearance of persons before the OPC and compel them to give oral or written evidence on oath and to produce any records and materials that the OPC considers necessary to investigate the complaint, in the same manner and to the same extent as a superior court of record; administer oaths;
- receive and accept any evidence and other information, whether on oath, by affidavit or otherwise, that the OPC sees fit, whether or not it is or would be admissible in a court of law;
- at any reasonable time, enter any premises, other than a dwelling-house, occupied by an organization on satisfying any security requirements of the organization relating to the premises; converse in private with any person in any premises entered under the fourth point above and otherwise carry out in those premises any inquiries that the OPC sees fit; examine or obtain copies of or extracts from records found in any premises entered under the fourth point above that contain any matter relevant to the investigation; and conduct audits of organizations if the OPC has reasonable grounds to believe that the organization has contravened a specific provision of PIPEDA.

Under PIPEDA, the OPC may attempt to resolve complaints by means of dispute resolution mechanisms, such as mediation or conciliation. In addition, the OPC may enter into compliance agreements whereby an organization agrees to bring itself into compliance with PIPEDA within a specified time period during which the OPC must not apply to the Federal Court for a hearing. An organization’s failure to live up to a commitment under a compliance agreement may result in an application to
Under the GDPR, supervisory authorities must also handle complaints lodged by data subjects and cooperate with data protection authorities from other countries.

Under the GDPR, supervisory authorities are tasked with promoting public awareness and understanding of the risks, rules, safeguards, and rights in relation to processing as well as promoting the awareness of controllers and processors of their obligations, amongst other tasks.

It is left to each Member State to establish a supervisory authority, and to determine the qualifications required to be a member, and the obligations related to the work such as duration of term as well as conditions for reappointment.

Under the GDPR, supervisory authorities have corrective powers which include:
- issuing warnings and reprimands;
- imposing a temporary or definitive limitation including a ban on processing;
- ordering the rectification or erasure of personal data; and
- imposing administrative fines.

the Federal Court requiring compliance with the agreement’s terms or seeing another order, penalty, or both.

Under PIPEDA, the OPC handles complaints lodged by individuals. Upon the findings of an investigation and the publication of a report of an investigation, the OPC may apply to the Federal Court for a hearing in respect of which a complaint was made or for matters referred to in an OPC report.

Under PIPEDA, the OPC is tasked with fostering public understanding and recognition of the purposes of PIPEDA as well as encouraging organizations to develop detailed policies and practices to comply with the protection of personal information and the breach of security safeguards.

Under PIPEDA, the OPC is the single federal supervisory authority and each province and territory designates its own supervisory authority under applicable privacy legislation.

Under PIPEDA, the corrective powers of the OPC are limited.

Differences
Under both laws, individuals have the right to lodge complaints with supervisory authorities, as well as courts. Under PIPEDA, an individual must first file a complaint with the OPC and after the OPC issues a report, the individual may apply to the Federal Court for a hearing. Under the GDPR, data subjects have the right to an effective judicial remedy if they consider that their rights have been infringed.

The GDPR provides individuals with a cause of action to seek compensation from a data controller and data processor for a violation of the GDPR. PIPEDA provides that the Federal Court may award damages to individuals.

Under the GDPR, the data subject has the right to lodge a complaint with the supervisory authority. The supervisory authority must inform the data subject of the progress and outcome of his or her complaint. Under PIPEDA, an individual has the right to file a written complaint with the OPC against an organization that contravened a provision in relation to the protection of personal information or breaches of security safeguards. If it is found that there are reasonable grounds to investigate a matter, the OPC may initiate a complaint. After the OPC issues a report of findings, the complainant may apply to the Federal Court for a hearing in respect of any matter in respect of which the complaint was made.

The GDPR provides that a data controller or processor must be exempt from liability to provide compensation if it proves that it is not in any way responsible for the event giving rise to the damage. PIPEDA does not include any provisions on exemption from liability for organizations.

The GDPR allows Member States to provide for the possibility for data subjects to give a mandate for representation to a body that has as its statutory objective the protection of data subject rights. PIPEDA does not address representation of complainants.

The GDPR contain an equivalent complaint report requirement, although supervisory authorities must inform data subjects of progress and outcomes of complaints. The OPC, within one year after the complaint, must prepare a report on the results of the complaint, containing:
• findings and recommendations;
• any settlement reached by parties;
• any determination and recommendation.
The GDPR does not explicitly define an equivalent set of remedies to be issued by courts. However, Member States may lay down rules on other penalties.

- if appropriate, a request that the organization give the OPC, within a specified time, notice of any action taken or proposed to be taken to implement the recommendations contained in the report or reasons why no such action has been or is proposed to be taken; and
- the recourse, if any, to be taken.

In addition to any other remedies, the Federal Court may order an organization to correct its practices, publish a notice of any action taken or proposed to be taken to correct its practices, and award damages.
INTRODUCING EKB

At EKB, our mission is to provide timely and practical advice to help our clients achieve the superior results they expect and deserve. When clients engage EKB, they can expect solid, exceptional service from lawyers who are leaders in their areas of practice. Our knowledge and wealth of experience enable us to offer focused, sound advice and innovative, practical solutions.

EKB offers strong expertise across a range of litigation and corporate commercial practice areas including:

- Business Law
- Business Litigation
- Commercial Lending & Finance
- Commercial Real Estate
- Construction & Builders Liens
- Employment Law
- Environmental
- Estate Planning & Litigation
- Financial Services
- Information & Privacy
- Mergers & Acquisitions
- Regulatory & Administrative Law
- Securities