Canadian Privacy Law Review

VOLUME 15, NUMBER 9 Cited as (2018), 15 C.P.L.R. AUGUST 2018

• PRIVACY COMMISSIONER ISSUES KEY GUIDELINES FOR CONSENT AND INAPPROPRIATE DATA PRACTICES •

Alex Cameron, Partner, Daniel Fabiano, Partner, and Robin Spillette, Summer Student, Fasken Martineau LLP

Alex Cameron

Daniel Fabiano

Robin Spillette

On May 24, 2018, the Office of the Privacy Commissioner of Canada published two important guidance documents in respect of activities regulated pursuant to the *Personal Information Protection and Electronic Documents Act* ("PIPEDA"):

- Guidelines for Obtaining Meaningful Consent (the "Consent Guidelines"), which includes a checklist for consent and is effective on January 1, 2019; and
- Guidance on Inappropriate Data Practices: Interpretation and Application of Subsection 5(3) effective on July 1, 2018 (the "Data Practices Guidance").

The publication of the above guidance documents comes on the heels of the Commissioner's consultation on consent and the recent updating of guidance on "Recording of Customer Telephone Calls". In this bulletin, we review the Consent Guidelines and Data Practices Guidance and highlight implications for organizations that are subject to PIPEDA.

• In This Issue •

LexisNexis®

CANADIAN PRIVACY LAW REVIEW

Canadian Privacy Law Review is published monthly by LexisNexis Canada Inc., 111 Gordon Baker Road, Suite 900, Toronto ON M2H 3R1 by subscription only.

ISBN 0-433-44417-7 (print) ISSN 1708-5446
ISBN 0-433-44650-1 (PDF) ISSN 1708-5454
ISBN 0-433-44418-5 (print & PDF)

Subscription rates: $325.00 per year (print or PDF)
$495.00 per year (print & PDF)

Please address all editorial inquiries to:

General Editor
Professor Michael A. Geist
Canada Research Chair in Internet and E-Commerce Law
University of Ottawa, Faculty of Law
E-mail: mgeist@uottawa.ca

LexisNexis Canada Inc.
Tel. (905) 479-2665
Fax (905) 479-2826
E-mail: cplr@lexisnexis.ca
Web site: www.lexisnexis.ca

GUIDELINES FOR OBTAINING MEANINGFUL CONSENT

The Consent Guidelines provide that organizations should follow seven key principles in seeking to obtain meaningful consent under PIPEDA. These are reviewed below.

1. Emphasize Key Elements

Emphasizing key elements in consent (and any associated public-facing privacy policy) can improve an individual's understanding of the consequences of giving consent, and thereby contribute to meaningful consent. The Consent Guidelines provide that organizations must generally put particular emphasis on the following elements:

a) What personal information is being collected, used and disclosed: Organizations should identify all information that will or may be collected, with sufficient precision to permit individuals to understand what they are consenting to.

b) The purpose for which the information is being collected, used or disclosed: Organizations should describe these purposes in sufficient detail to ensure that individuals have a meaningful understanding of them; vague descriptions should be avoided. Any purposes that are not integral to the provision of the organization's products or services, and any uses that would not be reasonably expected given the context, should be emphasized.

c) Information-sharing with third parties: Where organizations share information with a large number of third parties, or where the parties may change over time, an organization should list the types of organizations with which they are sharing information, and give users the ability to access more details if they desire. Any third parties that will be using the information for their own purposes, rather than for advancing the purposes of the first party, should be emphasized.

d) Whether there is a risk of harm arising from the collection, use or disclosure of information: Organizations should consider emphasizing harms that may be associated with the activity for

which consent is sought, including both direct as well as indirect harms (*e.g.*, unauthorized use of information). The risk of harm refers to any risk of significant harm (that is, more than minimal or a mere possibility) after accounting for any mitigating procedures taken by the organization. Individuals must be aware of the consequences of their consent in order for that consent to be meaningful. This includes indirect risks, such as third party misuse of information.

2. Allow Individuals to Control the Level of Detail

Organizations should make privacy disclosures more manageable and accessible by allowing individuals to decide how, when, and how much information about an organization's privacy practices the individual accesses at any given time. Layered disclosure is one such approach. Layered disclosure starts by displaying more abstracted, general information, and allows individuals to obtain more detail on discrete topics if they wish. Additionally, privacy disclosures should be readily available so that an individual can return and re-read about an organization's privacy practices. This approach supports meaningful consent, as it allows individuals an opportunity to reconsider and potentially withdraw consent if they object to any of the organization's practices.

3. Provide Individuals with Clear Options to say 'Yes' or 'No'

Organizations must not require individuals to consent to the collection, use or disclosure of more information than is necessary for the product or service which is being provided. For a collection, use, or disclosure to be "necessary", it must be integral to the provision of that product or service (*i.e.*, required to fulfill the explicitly specified and legitimate purpose). If any other information is to be collected on an opt-in or opt-out basis, individuals should be able to choose whether or not to consent to the collection of this additional information, and this choice should be clear and accessible, unless an exception to consent applies.

4. Be Innovative and Creative

Organizations should think about moving away from simply transposing paper-based policies into their digital environments, and seek innovative ways to obtain consent. "Just-in-time" notices, for example, are an alternative to obtaining all consents "up-front". For example, a cell phone application that, rather than asking for access to location data upon installation, asks for this consent the first time the individual attempts to use the application in a way which requires location data, provides more context to the individual and a better understanding of what is being collected and why. Other interactive tools such as videos, or click-through presentations which explain privacy policies, and mobile interfaces, could also be used. Additional information regarding mobile apps is provided in the Commissioner's guidance: "Seizing Opportunity: Good Privacy Practices for Developing Mobile Apps".

5. Consider the Target Individual's Perspective

To ensure that consents and privacy disclosures are user-friendly and understandable, organizations must be mindful of the perspective of target individuals. This involves the use of an appropriate level of language, clear explanations and a comprehensible display. It also involves consideration of the types of devices that target individuals will be using (laptops, mobile phones, tablets, etc.). Organizations may wish to understand the perspective of target individuals by consulting with them, running pilot tests and focus groups, engaging with privacy experts and following industry best-practices.

6. Make Consent a Dynamic and Ongoing Process

Consent should be an ongoing, dynamic and interactive process (and not a one-off process). Periodic reminders and refreshers about an organization's privacy practices should be implemented, as well as an ongoing and practical ways for individuals to obtain more information.

7. Be Accountable: Stand Ready to Demonstrate Compliance

Organizations should be ready to prove that they have obtained meaningful consent, including showing that their consent process is understandable and accessible. One such way to do this is for organizations to be aware of these guidelines, as well as the guidance provided by the Commissioner in "Getting Accountability Right with a Privacy Management Program", and to show that they have followed them.

ADDITIONAL TOPICS ADDRESSED IN THE CONSENT GUIDELINES

Appropriate form of Consent

In addition to the seven guiding principles above, the Guideline reminds organizations of the need to consider what type of consent is appropriate given the circumstances. While in some situations implied consent may be adequate, there are some circumstances which will generally require express consent, including: (a) when the information being collected, used or disclosed is sensitive in nature; (b) when an individual would not reasonably expect certain information to be collected, used or disclosed given the circumstances, and (c) when there is a more than minimal risk of significant harm.

CONSENT AND CHILDREN

Another contextual factor is whether the target individuals include children. When children are involved, organizations should take into account the fact that children will generally have different emotional and cognitive processing abilities than adults. This affects their ability to understand how their personal information is being used, and hence will affect their ability to give meaningful consent. The OPC requires that, for children 13 and under, a parent or guardian give consent on the child's behalf. When the target individuals include minors who are able to provide consent themselves, organizations should still take their maturity into account, and should be ready to show how they have done so.

At the conclusion of the Consent Guidelines, the Commissioner provides a useful checklist of "Should do" and "Must do" action items for organizations seeking to obtain meaningful consent under PIPEDA.

GUIDANCE ON INAPPROPRIATE DATA PRACTICES

Concurrently with publishing the Guidelines, the Commissioner published the Data Practices Guidance, which sets out various considerations that organizations should keep in mind when assessing whether a certain practice may be contrary to subsection 5(3) of PIPEDA.

Subsection 5(3) of PIPEDA is an overarching requirement which provides that: "An organization may collect, use or disclose personal information only for purposes that a reasonable person would consider appropriate in the circumstances." In order words, even with an individual's consent, there are certain purposes that would be unacceptable under PIPEDA on the grounds that a reasonable person would not consider them to be appropriate.

Like meaningful consent, whether or not a purpose is inappropriate requires a contextual approach. As summarized in the Data Practices Guidance, the following factors have been applied by the Commissioner and the courts:

- Whether the organization's purpose represents a legitimate need / bona fide business interest;
- Whether the collection, use and disclosure would be effective in meeting the organization's need;
- Whether there are less invasive means of achieving the same ends at comparable cost and with comparable benefits; and
- Whether the loss of privacy is proportional to the benefits (which includes consideration of the degree of sensitivity of the personal information at issue).

In addition, as set forth in the Data Practices Guidance, the Commissioner has established a list of prohibited purposes under PIPEDA, which they

have deemed "No-Go Zones". The Commissioner considers that a reasonable person would not consider the collection, use or disclosure of information to be appropriate in these circumstances. Currently, the list of "No-Go Zones" may be summarized as follows:

- Collection, use or disclosure that is otherwise unlawful (*e.g.*, violation of another law);
- Collection, use or disclosure that leads to profiling or categorization that is unfair, unethical or discriminatory in a way which is contrary to human rights law;
- Collection, use or disclosure for purposes that are known or likely (on a balance of probabilities) to cause significant harm to the individual (*e.g.*, bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, identity theft, negative effects on credit record or damage to or loss of property);
- Publishing personal information with the intended purpose of charging individuals for its removal (*i.e.*, "blackmail");
- Requiring passwords to social media accounts for the purpose of employee screening; and
- Surveillance by an organization through the use of electronic means (*e.g.*, keylogging) or audio or video functionality of the individual's own device.

While these "No-Go Zones" are important to note, organizations should also remember that the list is not binding, determinative or exhaustive, and that subsection 5(3) requires a contextual analysis. What a reasonable person would consider appropriate is a flexible and evolving concept which will be revisited by the Commissioner from time to time.

IMPLICATIONS FOR ORGANIZATIONS SUBJECT TO PIPEDA

The Commissioner's guidance documents do not have the force of law and are not binding on organizations. However, they plainly set out the Commissioner's expectations, provide a benchmark against which the Commissioner will assess practices in the context of a complaint, audit or investigation, and provide a useful reference for organizations seeking to comply with PIPEDA.

It is also important to note that, over time, previous Commissioner guidance documents, including "Guidelines for Processing Personal Data Across Borders", have come to set the *de facto* standard and practices under PIPEDA. Organizations should familiarize themselves with the new guidance documents and consider steps to amend practices as necessary. For example, organizations which use mobile and online interfaces can refer to work which is already being done regarding the implementation of privacy icons, and privacy dashboards to help obtain meaningful consent. These and other potential solutions are discussed in the Commissioner's discussion paper, "Consent and Privacy".

Finally, in considering compliance with the new guidelines discussed in this bulletin, organizations should be mindful of the consequences of failing to obtain meaningful consent or failing to process information for appropriate purposes as required by PIPEDA. For example, a failure to obtain meaningful consent from a large number of individuals could undermine the basis upon which key business operations are premised. This could not only render those operations non-compliant with PIPEDA but also give rise to class action litigation risk for a privacy breach (*e.g.*, processing personal information for commercial purposes without adequate consent).

• UNDERSTANDING THE GDPR: A COMPARISON BETWEEN THE GDPR, PIPEDA AND PIPA •

J. Sébastien A. Gittens, Partner and Trademark Agent, Bennett Jones LLP, Stephen D. Burns, Partner, Trademark Agent, Head of Intellectual Property, Bennett Jones LLP, Martin P.J. Kratz QC, FCIPS, Partner, Trademark Agent, Bennett Jones LLP, Kees de Ridder, Articling Student, Bennett Jones LLP, Danielle Miller Olofsson, BCF LLP

J. Sébastien A. Gittens

Stephen D. Burns

Martin P.J. Kratz QC

Danielle Miller Olofsson

The European Union's *General Data Protection Regulation* (the "**GDPR**") came into force on May 25, 2018. To assist Canadian organizations with their potential compliance efforts with respect to same, the following is intended to provide a non-exhaustive, high-level comparison between: (i) the GDPR; (ii) Canada's *Personal Information Protection and Electronic Documents Act* ("**PIPEDA**"); (iii) Quebec's *Act Respecting the Protection of Personal Information in the Private Sector* ("**PPIPS**"); together with (iv) the *Personal Information Protection Acts* of Alberta and British Columbia (collectively, the "**PIPAs**"). While there are important nuances to each of these regulatory frameworks, they broadly draw on fair information practices that result in substantial commonality among them. In fact, a number of elements in Canadian private sector privacy law, especially in the PIPAs, have anticipated some provisions in the GDPR.

	GDPR	PIPEDA	PIPAs	PPIPS
Who does it apply to?	The GDPR applies to natural or legal person, public authority, agency or other body that has an establishment in the EU. The GDPR has extraterritorial effect; it applies to any natural or legal person, public authority, agency or other body outside of the EU who: • targets individuals in the EU by offering goods or services (regardless of whether a payment is required); or • monitors the behavior of individuals in the EU (where that behavior takes place in the EU).	PIPEDA applies to: • the collection, use and disclosure of personal information by an organization in the course of its commercial activity in a province without substantially similar privacy legislation; • the transfer of personal information across borders; • federal works, undertakings or businesses ("**FWUBs**"); and • the collection, use and disclosure of employee information in connection with FWUBs. Certain jurisprudence has held that PIPEDA has extraterritorial application when, for example, there is a "real and substantial connection" between Canada and the activity undertaken in a foreign jurisdiction. PIPEDA does not apply to provincial statutes that have been deemed to be substantially similar to PIPEDA.	The PIPAs applies to the collection, use and disclosure of personal information by an organization that occurs within Alberta/ BC. The Alberta PIPA only applies to non-profit organizations in respect of their commercial activities. The PIPAs have been deemed to be substantially similar to PIPEDA.	PPIPS applies to a person that collects, holds, uses or communicates personal information to a third party in the course of carrying out an organized economic activity consisting of producing, administering or alienating property or providing services. This economic activity does not have to be commercial in nature and therefore PPIPS applies to non-profit organizations. PPIPS has been deemed to be substantially similar to PIPEDA.

	GDPR	PIPEDA	PIPAs	PPIPS
What does it apply to?	The GDRP applies to "personal data", namely "any information relating to an identified or identifiable natural person … ; 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 applies to "personal information", namely "information about an identifiable individual" (other than business contact information of an individual that an organization collects, uses or discloses solely for the purpose of communicating or facilitating communication with the individual in relation to their employment, business or profession).	The PIPAs apply to "personal information", namely "information about an identifiable individual". There are various exemptions under each of the PIPAs. For example: • Alberta's PIPA does not apply to: (i) the collection, use or disclosure of an individual's business contact information if the collection, use or disclosure, as the case may be, is for the purposes of enabling the individual to be contacted in relation to the individual's business responsibilities and for no other purpose; or (ii) personal health information; and • BC's PIPA does not apply to: (i) information to enable an individual at a place of business to be contacted; or (ii) information prepared or collected as a part of the individual's responsibilities or activities related to the individual's employment or business (but does not include personal	PPIPS applies to "personal information" which is defined as "information which relates to a natural person and allows that person to be identified". PPIPS does not apply to "journalistic, historical or genealogical material collected, held, used or communicated for the legitimate information of the public".

	GDPR	PIPEDA	PIPAs	PPIPS
			information about an individual who did not prepare or collect the personal information).	
Consent	Consent means any freely given, specific, informed and unambiguous indication of an individual's wishes which, by a statement or by a clear affirmative action, signifies an agreement to the processing of their personal data. The GDPR provides that there are exceptions from the requirement for consent in certain circumstances.	The knowledge and consent of an individual are generally required for the collection, use, or disclosure of their personal information. Any such consent is only valid if it is reasonable to expect that an individual would understand the nature, purpose and consequences of the collection, use or disclosure of the personal information to which they are consenting. PIPEDA recognizes that consent may be implied in certain cases and that consent can be deemed in some specific circumstances. PIPEDA also provides that there are exceptions from the requirement for consent in certain circumstances.	The Alberta and BC Privacy Commissioners have held that consent must be "meaningful" (*i.e.*, an individual must understand what an organization is doing with their information). On or before collecting personal information about an individual, an organization must disclose to the individual verbally or in writing: (i) the purposes for the collection of the information; and (ii) the position name or title and the contact information of a person who is able to answer the individual's questions about the collection. The PIPAs recognize that consent may be implied in certain cases and that consent can be deemed in some specific circumstances. The PIPAs also provide that there are exceptions from the requirement for consent in certain circumstances.	PPIPS requires consent to be manifest, free and enlightened. It must be given for a specific purpose and is only valid for the length of time needed to achieve the purpose for which it was requested. When an organization collects personal information about an individual, it must inform the individual of the object of the file, the use to be made of the information, the categories of people who will have access to the information, the place where it will be kept and the individual's rights of access and rectification. PPIPS allows for situations in which consent is not required such as in the case of an emergency affecting the person's health or safety or for law enforcement purposes.

	GDPR	PIPEDA	PIPAs	PPIPS
Data Protection	Personal data must be processed in a manner that "ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures". Such measures must be designed to implement data-protection principles in an effective manner and to integrate the necessary safeguards.	Appropriate to the sensitivity of the information, an organization must adopt security safeguards to protection the personal information in its custody and control against loss or theft, as well as unauthorized access, disclosure, copying, use or modification. Methods of protections must include physical, organizational and technological measures.	An organization must protect personal information that is in its custody or under its control by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure, copying, modification, disposal or destruction.	PPIPS requires the person collecting, using, communicating, storing or destroying personal information to take the security measures necessary to ensure the protection of the information. These measures must be reasonable given the sensitivity of the information, the purposes for which it is to be used, the quantity and distribution of the information and the medium on which it is stored.
Accountability	Appropriate technical and organizational measures must be implemented to ensure and to be able to demonstrate that processing is performed in accordance with the GDPR. This may include the implementation of appropriate data protection policies, and adherence to applicable "codes of conduct" and "certification mechanisms". In certain circumstances, a controller or processor must designate a "representative" in the EU (*i.e.*, a natural or legal person established in the EU who represents a controller or processor	An organization is responsible for any personal information under its control and must designate one or more individuals who are accountable for the organization's privacy compliance. Organizations must implement applicable policies and practices to give effect to PIPEDA, including: • "implementing procedures to protect personal information; • establishing procedures to receive and respond to complaints and inquiries;	An organization is responsible for any personal information under its custody and control, and must designate one or more individuals who are responsible for the organization's privacy compliance. Organizations must implement applicable policies and practices to give effect to the PIPAs. An organization must make written information about its privacy policies and practices available on request.	An organization is responsible for any personal information under its custody and control, and must designate one or more individuals who are responsible for the organization's privacy compliance. Organizations must implement applicable policies and practices to give effect to PPIPS.

	GDPR	PIPEDA	PIPAs	PPIPS
	with regard to their respective obligations under GDPR). In certain instances, a "data protection officer" must also be appointed.	• training staff and communicating to staff information about the organization's policies and practices; and • developing information to explain the organization's policies and procedures".		An organization must make written information about its privacy policies and practices available on request.
Individual Rights	The GDPR includes the following rights for individuals: • the right to access their personal information (together with additional information such as the purposes of the processing, the recipients to whom the personal data have been or will be disclosed, and the source of their personal information); • the right to have their personal information be accurate and, where necessary, kept up to date; • the right to rectification (*i.e.*, with respect to the correction of inaccurate personal data); and • the right to withdraw their consent at any time.	PIPEDA includes the following rights for individuals: • the right to access their personal information under the custody or control of an organization; • the right to have their personal information be accurate, complete and up-to-date (as is necessary for the purposes for which it is to be used); • the right to have their personal information amended (by the correction, deletion, or addition of information) when an individual successfully demonstrates the inaccuracy or incompleteness of their personal information; and	The PIPAs include the following rights for individuals: • the right to access their personal information under the custody or control of an organization; • the right to know the purposes for which their information has been and is being used; • the right to request a correction to any error or omission in respect of their personal information, when an individual successfully demonstrates the inaccuracy or incompleteness of their personal information; and • the right to withdraw or vary their consent at any time, subject to legal or contractual restrictions and reasonable notice.	PPIPS includes the following rights for individuals: • Right to have the personal information that has been collected communicated to them • Right to have any personal information collected otherwise than according to the law deleted • Right to know where the personal information is held and whom to contact for more information • Right to have personal information removed from a nominative list that is to say a list

	GDPR	PIPEDA	PIPAs	PPIPS
	Additional rights include: • the right to erasure (also known as the right to be forgotten); • the right to data portability (namely, the ability to receive the personal data in a structured, commonly used and machine-readable format and have such data transmitted to another controller); • the right to restriction of processing (*e.g.*, if the accuracy of the personal data is contested by the individual); and • the right not to be subject to automated decision-making.	• the right to withdraw their consent at any time, subject to legal or contractual restrictions and reasonable notice.		of clients, members or employees used for philanthropic or commercial prospection A decision by the Quebec Privacy Commission (the "**Commission**") suggests that Quebec does not necessarily recognise the right to forget.
Cross-border Processing	Generally, an organization may transfer personal data to a third party service provider outside of the EU in limited circumstances, including: • the non-EU country has been held by the Commission to provide an "adequate level of protection" with respect to personal data; • if appropriate safeguards are provided for, and on condition that enforceable rights and effective legal remedies for individuals are available, by way of: (i) "binding corporate rules";	Generally, an organization may transfer personal information to a third party service provider in a jurisdiction outside of Canada if the organization: (i) is satisfied that the service provider has policies and processes in place to ensure that the information in its care is properly safeguarded at all times(including training for its staff and effective security measures); (ii) uses contractual or other means to "provide a comparable level of protection while the information is being processed by	Generally, Alberta's PIPA provides that an organization may transfer personal information to a third party service provider in a jurisdiction outside of Canada if the organization's policies and practices include information regarding: (i) the countries outside Canada in which such activities may occur; and (ii) the purpose for which the service provider has been authorized to collect, use or disclose personal information. An organization must make written information available about these policies and practices. Notice must also be	PPIPS requires persons sending personal information outside Quebec to make sure that the information receives the same protection it would under Quebec law.

	GDPR	PIPEDA	PIPAs	PPIPS
	(ii) standard data protection clauses adopted by the Commission; (iii) an approved "code of conduct"; or (iv) an approved "certification mechanism"); or • if appropriate safeguards are provided for by contractual clauses (with the recipient of the personal data in the non-EU country) that are authorized by a competent supervisory authority in the EU.	the third party"; (iii) has the right to audit and inspect how the third party handles and stores personal information; and (iv) at the time that the personal information is collected from an individual, makes it plain that their information may be processed in a foreign country and that it may be accessible to law enforcement and national security authorities of that jurisdiction.	given, before or at the time of collecting or transferring the personal information, of: (i) the way in which the individual may obtain access to written information about the organization's policies and practices with respect to service providers outside Canada; and (ii) the name or title of a person who is able to answer questions about the collection, use, disclosure or storage of personal information by service providers outside Canada. BC's PIPA does not explicitly address the transfer personal information to a third party service provider in a jurisdiction outside of Canada. Nevertheless, this statute appears to contemplate same by the fact that an organization is "responsible for personal information under its control, including personal information that is not in the custody of the organization".	
Data Breach Notifications	A data controller must: • notify the applicable supervisory authority of a personal data breach that is likely to result in a risk to the rights and freedoms of natural persons; and	Commencing on November 1, 2018, an organization must: • report to the federal Privacy Commissioner any breach of security safeguard involving personal	Since 2010, Alberta's PIPA states that an organization must provide notice to the Alberta Privacy Commissioner of any incident involving the loss of or unauthorized access to or disclosure	Although there are no data breach notification requirements specifically set out in PPIPS, the Commission strongly encourages

	GDPR	PIPEDA	PIPAs	PPIPS
	• notify an individual of a personal data breach involving the individual's personal data that is likely to result in a high risk to the rights and freedoms of said individual.	information under its control if it is reasonable in the circumstances to believe that the breach creates a real risk of significant harm to an individual; and • notify an individual of any breach of security safeguards involving the individual's personal information if it is reasonable in the circumstances to believe that the breach creates a real risk of significant harm to the individual.	of the personal information if there is a real risk of significant harm to an individual as a result of the loss or unauthorized access or disclosure. The Privacy Commissioner may require the organization to notify affected individuals. BC's PIPA does not explicitly have any breach reporting obligations.	organizations that have been subject to a breach to notify the Commission as well as the people whose information has been compromised. The Commission's site includes breach notification forms to facilitate such a disclosure.
Data Protection Authority	Each supervisory authority has various: • investigative powers (*e.g.*, to carry out data protection audits); • corrective powers (*e.g.*, (i) to issue warnings and reprimands; (ii) to order an organization to bring processing operations into compliance with the provisions of the GRPR; and (iii) to order an organization to communicate a data breach to affected data subjects); and	Under PIPEDA, the federal Privacy Commissioner can make non-binding recommendations to organizations, but cannot issue binding orders or impose administrative monetary penalties.	The Alberta and BC Privacy Commissioners have the authority to make various orders, including, for example: • directing an organization to give an individual access to their personal information; • confirming a decision of an organization regarding access to an individual's personal information; • directing an organization to refuse to give an individual access to their personal information;	The Commission: • hears access to information complaints, makes orders and imposes fines; • conducts inquiries either on its on initiative or in response to a complaint; and • advises organizations to comply or refuse to comply with access to information requests

	GDPR	PIPEDA	PIPAs	PPIPS
	• advisory powers (*e.g.*, (i) to accredit certification bodies; (ii) to adopt standard data protection clauses; and (iii) to approve binding corporate rules),		• requiring that a duty imposed by PIPA be performed; or • requiring an organization to destroy personal information collected in contravention of PIPA.	
Administrative Fines and Penalties	Depending on the circumstances, administrative fines of up to: • €20 million; or • 4% of annual worldwide turnover (whichever is higher).	Fines of up to $100,000 can be imposed by the Federal Court in three circumstances: (i) if an organization dismisses, suspends, demotes, disciplines, harasses or otherwise disadvantages an employee who acted as a "whistle blower"; (ii) if an organization does not retain personal information that is the subject of a request for as long as is necessary to allow the individual to exhaust any recourse that they may have; or (iii) if a person obstructs the federal Privacy Commissioner in the investigation of a complaint or in conducting an audit.	An individual or organization who commits an offence under PIPA is liable to a fine of up to $10,000 and $100,000, respectively. Under Alberta's PIPA, such a fine can arise if, for example, an organization: (i) collects, uses or discloses personal information in contravention of Alberta's PIPA; (ii) attempts to gain or gains access to personal information in contravention of Alberta's PIPA; (iii) makes an adverse employment action against an employee who acted as a "whistle blower"; or (iv) fails to comply with an order made by the Alberta Privacy Commissioner. Under BC's PIPA, such a fine can arise if, for example, an organization: (i) uses deception or coercion to collect personal information; (ii) disposes of personal	PPIPS provides for a variety of penalties, the most relevant of which are: $1,000 to $10,000 and $10,000 to $20,000 for a subsequent offense for a person that collects, holds, communicates to third persons or uses personal information on other persons in violation of PPIPS; $5,000 to $50,000 and $10,000 to $100,000 for a subsequent offense for a person that transfers information to a jurisdiction that does not have personal information safeguards that are at least as strict as Quebec; and $1,000 to $10,000 and $2,000 to $20,000 for a subsequent offense to any person

	GDPR	PIPEDA	PIPAs	PPIPS
			information with an intent to evade a request for access; (iii) dismisses, suspends, demotes, disciplines, harasses or otherwise disadvantages an employee who is a whistleblower; or (iv) fails to comply with an order made by the BC Privacy Commissioner.	that hampers an inquiry or inspection by communicating false or inaccurate information It should be noted that a directing mind or legal representative of a legal person who ordered or authorized the act or omission that constitutes the violation will be considered a party to the offense and liable to the prescribed penalty.
Private Right of Action	Each data subject will have the right to: (i) an "effective judicial remedy" where he or she considers that his or her rights under this GDPR have been infringed; and (ii) receive compensation for any material or non-material damage arising from any such infringement.	In certain circumstances, the Federal Court may order an organization to correct its privacy practices and award damages to a complainant.	An individual has a cause of action against an organization for damages if: (i) the Alberta or BC Privacy Commissioner has made an order against the organization; or (ii) a person has been convicted of an offence under PIPA, and the organization has no further right of appeal in either instance.	An individual who is not happy with a decision by an organization regarding their personal information or who believes PPIPS to have been violated may bring a complaint before the commission. The commission has the authority to render decisions which become enforceable once homologated by the Superior Court. Appeal may be made before the Court of Quebec.