Office of the
Information &
Privacy Commissioner
for British Columbia

Protecting privacy. Promoting transparency.

GUIDANCE DOCUMENT

COMPETITIVE ADVANTAGE: COMPLIANCE WITH PIPA AND THE GDPR

MARCH 2018

CONTENTS

PURPOSE OF THIS GUIDANCE DOCUMENT

The *Personal Information Protection Act* (PIPA)[1] applies to all private sector organizations in British Columbia and sets out how those organizations may collect, use, and disclose personal information.

Effective May 25, 2018, some organizations subject to PIPA must also comply with the European Union (EU) General Data Protection Regulation (GDPR).[2] The GDPR applies to organizations that have an established presence in the EU, offer goods and services to individuals in the EU, or monitor the behaviour of individuals in the EU. Organizations that do not comply with the GDPR face significant fines.

This guidance helps organizations in BC determine whether they are subject to the GDPR and explains how to comply with both PIPA and the GDPR.

ORGANIZATIONS SUBJECT TO PIPA

- Corporations and strata corporations
- Partnerships
- Doctors' offices
- Unincorporated associations
- Co-operative associations
- Societies
- Churches and other religious organizations
- Charities and not-for-profits
- Sports clubs
- Trade unions
- Partnerships
- Political parties
- Individuals involved in a commercial activity
- Trusts

QUICK REFERENCE GUIDE: GDPR VS BC PIPA

TOPIC	GDPR	BC PIPA	ADVICE
Scope	Obligations whenever personal data is processed.	Obligations whenever personal data is collected, used, or disclosed.	PIPA and the GDPR are equivalent. Comply with either.
Personal information/data	Information relating to identified or identifiable natural person.	Information about an identifiable individual.	
Consent	Does not permit opt-out consent. Special consent, explicit consent, consent for minors.	Permits opt-out consent. Express consent, deemed consent. Measured on a level of reasonableness.	The GDPR is more protective than PIPA. Compliance with GDPR would ensure compliance with PIPA.
Processing personal data without consent	Permitted if several conditions are met. Businesses can process without consent for legitimate business interests.	Permitted for employee personal information and in other limited circumstances.	The GDPR and PIPA are different. Compliance with one would not ensure compliance with the other.
Individual rights	• right to be informed • right to access • right to correction of personal information • right to erasure • right to restriction of processing • right to data portability • right to object to data processing activities • right to logic behind automated decision making	• right to be informed • right to access personal data • right to request correction of personal information	The GDPR has more robust individual rights. Compliance with the GDPR will ensure compliance with PIPA.
Mandatory breach notification	Notification required within 72 hours.	Notification is not required, but is a best practice.	The GDPR is more protective than PIPA. Compliance with GDPR will ensure compliance with PIPA.
Cross-border transfers of personal information	Permits organizations to transfer personal data outside the EU in some cases (e.g.: adequacy).	Not addressed in legislation.	
Data governance obligations	Organizations must implement technical and organizational measures to show compliance.	Requires organizations to protect and secure personal information.	
Privacy impact assessments	Mandatory before initiating any processing with high risk of infringing on individual rights.	Recommended, but not required.	
Data protection officer	Required for large-scale processing.	Required.	At a minimum, designate a person responsible for privacy.
Sanctions	Serious infringement: up to 20m Euros or 4% of annual worldwide turnover. Lesser infringement: up to 10m Euros or 2% of annual worldwide turnover.	Individual: up to $10k. Organization: up to $100k	The GDPR has much higher fines than PIPA.

1.0 INTRODUCTION

On May 25, 2018 the EU GDPR came into force, repealing the existing Directive 95/46/EC (Directive) and requiring private sector organizations to comply with new data protection requirements when they process the personal information of individuals located in the EU. The GDPR applies to both the private and public sectors, but this guidance only considers the implications for private sector organizations in BC.

The GDPR has two broad sections. The first section contains 173 recitals that provide context, direction, and guidance for the second section of the GDPR, which contains 99 articles divided into 11 chapters. The articles set out the specific requirements of the GDPR and are legally binding; the recitals inform the interpretation of the articles, but are not legally binding.

The GDPR sets a new, higher standard for global privacy legislation. It harmonizes data privacy laws across Europe, gives greater privacy protection and rights to individuals,[i] and extends the reach of personal data protection beyond the borders of the EU. It also imposes significant new obligations on BC organizations that process the personal data of EU data subjects.[3]

The reach of the GDPR presents global compliance challenges for organizations in BC. Organizations covered by PIPA will also need to comply with the GDPR if:

1. they have an established presence in the EU;
2. they offer goods and services to individuals in the EU; or
3. they monitor the behaviour of individuals in the EU.[4]

PIPA and the GDPR are similar, giving PIPA-compliant organizations in BC a head start toward GDPR compliance. However, some aspects of the GDPR have no equivalent in PIPA, so additional effort will be required in those areas. The GDPR is an incentive for organizations to implement strong data protection practices.

1.2 Controllers and processors

The GDPR applies when personal data is "processed." The GDPR defines processing as "any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, 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."[5]

[i] The UK introduced a new Data Protection Bill on September 03, 2017, which is substantially similar to the GDPR. Once the UK leaves the EU the GDPR will no longer apply, but the Data Protection Bill, which will eventually evolve into the Data Protection Act 2018, constantly cross-references the GDPR and is substantially very similar.

The GDPR defines any entity that collects, uses, or discloses personal information of EU residents as a "controller" or a "processor." A controller refers to "the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data."[6] A processor means any person, public authority or agency that processes personal data on behalf of the controller.[7]
As noted above, the GDPR applies to any controller or processor of personal data of EU data subjects, whether or not the processing takes place in the EU, and whether or not the controller or processor operates or has offices in the EU.

1.3 Fundamental principles for processing personal data

According to the GDPR, processing of personal data must be in accordance with the principles of lawfulness, fairness, and transparency.[8] Organizations must explicitly specify legitimate purposes for collecting personal data, and that data must only be processed in a way that is compatible with those purposes.[9]

Data controllers or processors must also respect the principle of data minimization, meaning that the processing of personal data must be limited to that which is adequate, relevant, and necessary to achieve the specified purpose.[10]

Personal data must be accurate, kept up to date,[11] kept in a form which permits identification of data subjects for no longer than is necessary, and must be processed in a manner that ensures appropriate security of the personal data.[12]

ADVICE FROM THE COMMISSIONER	"Processing" under the GDPR is the same as "collection, use, or disclosure" under PIPA.
	Assess whether your organization falls within the scope of the GDPR: Any organization that has customers in the EU, operates in the EU, or collects, uses, or discloses personal information of EU data subjects should ensure compliance prior to May 25, 2018.

2.0 PERSONAL INFORMATION

2.1 Personal information » GDPR

The GDPR defines personal data as any information relating to an identified or identifiable natural person (often referred to as a "data subject"). An identifiable natural person is one who can be identified, directly or indirectly, by reference to an identifier such as a name, an identification number, location data, an online identifier such as an IP address, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that person.[13]

The GDPR sets out special categories of particularly sensitive personal data that is subject to additional protections: data that reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership; data concerning health or sex life and sexual orientation; genetic data or biometric data. The GDPR provides specific restrictions for processing special personal data. Processing is only allowed under certain circumstances, such as if the data subject has given explicit consent for specified purposes. In other circumstances, consent cannot be the authority for the processing of sensitive data. [14]

Pseudonymization is a technique for processing personal data so that it cannot be attributed to a specific data subject without additional information. The GDPR requires that the additional (re-identifying) information be stored separately from the pseudonymized data and protected with technical and organizational measures to ensure that the personal information is not attributed to an identified or identifiable natural person.[15] Pseudonymized information is still a form of personal data,[16] but this technique is recommended as a safeguard to reduce risk of a privacy breach..[17]

2.2 Personal information » PIPA

PIPA defines personal information as "information about an identifiable individual," which can include name, date of birth, phone number, address, physical description, social insurance number, personal financial information, and more. It does not include employee contact information or work product information.[18] PIPA does not have a separate definition for sensitive or "special" personal information.

ADVICE FROM THE COMMISSIONER	
	Make sure your organization is aware of the GDPR's special categories of sensitive personal information, and ensure that these categories receive additional protection.
	Consider using pseudonymization techniques, but remember that pseudonymized data still requires protection as a form of personal data.

3.0 CONSENT

3.1 Consent » GDPR

The GDPR has stronger consent requirements for information processing than those required by PIPA.[19]

Under the GDPR, "consent" of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by a statement or clear affirmative action agreeing to the processing of their personal data.[20] The GDPR does not permit opt-out consent.[21]

Specific consent is required for any new data processing, unless the subsequent processing is so similar to those already consented to that it would be expected by the data subject.[22] Organizations are only allowed to offer services or products conditional on consent if the data processing is necessary to provide the service or product.[23] Organizations must allow users to withdraw consent, and they must inform users of this right. Most notably, consent must be as easily revoked as it is given.[24]

The GDPR requires explicit consent for the processing of special categories of data,[25] for automated individual decision-making, including profiling,[26] and for international data transfers.[27]

The requirements for explicit consent are set out in the GDPR's definition of consent at Article 4(11). Explicit consent can be obtained in a clear written or spoken statement that leaves no room for misinterpretation. The GDPR suggests two-stage verification for explicit consent as a best practice.

The Article 29 Working Party has developed *Guidelines on Consent*,[28] which give this example of explicit consent in the scope of sensitive personal data: "A clinic for cosmetic surgery seeks explicit consent from a patient to transfer his medical record to an expert whose second opinion is asked on the condition of the patient. The medical record is a digital file. Given the specific nature of the information concerned, the clinic asks for an electronic signature of the data subject to obtain valid explicit consent and to be able to demonstrate that explicit consent was obtained."[29]

3.1.1 Consent » GDPR » Imbalance of Power

The GDPR recognizes that when there is a clear imbalance of power in the relationship between the controller and the data subject, consent is not likely a sufficient authority for data processing.[30] In the private sector, an imbalance of power can occur in the employment and housing rental contexts. An employee or tenant cannot easily deny consent to data processing by their employer or landlord without jeopardizing their job or housing. Employers and landlords should therefore rely on other lawful bases to process the personal data of their employees or tenants, as discussed in section 4.0.[31]

3.1.2 Consent » GDPR » Children

Children have specific protections for their personal data in the GDPR.[32] The processing of personal data of any child under 16 requires parental consent, though member states can opt to reduce the age to 13, 14, or 15.[33] The controller must ensure that communication to the data subject is concise, transparent, intelligible, and easily accessible, using clear and plain language, particularly for any information addressed specifically to a child.[34]

3.2 Consent » PIPA

PIPA also requires an organization to obtain consent before collecting, using, or disclosing personal information about an individual, but PIPA's requirements are slightly different.

In addition to express consent,[35] PIPA recognizes:

- Implicit consent, when an individual volunteers information for an obvious purpose and a reasonable person would consider it appropriate for the individual to volunteer that information in those circumstances;[36]
- "Opt-out consent," such as a pre-checked box where consent is presumed but can be declined;[37]
- The right to withdraw or change consent;[38] and
- The collection, use, or disclosure of personal information without consent or from another source in certain situations.[39]

Under PIPA, in addition to consent, any collection, use, or disclosure of personal information must be reasonable.[40] This means that a reasonable person, knowing the purpose for collection and the surrounding circumstances, would consider the purpose to be appropriate. What is reasonable depends on the sensitivity and volume of personal information being collected, the purpose and circumstances of collection, how the organization handles the information, and how an organization plans to use and disclose the information.[41]

Similar to the GDPR, PIPA only allows an organization to require consent in order to provide a product or service where the collection, use, or disclosure of personal information is "necessary" or integral to the provision of the product or service.[42,43]

3.2.1 Consent » PIPA » Imbalance of Power

PIPA does not explicitly address the effect of an imbalance of power on validity of consent. However, PIPA recognizes that the employment relationship is not voluntary by stating that "employee personal information" may be collected, used, or disclosed without consent when it is reasonable for establishing, managing, or terminating the employment relationship. The employer must notify the employee of the purpose for collecting, using, or disclosing employee personal information prior to collection, use, or disclosure. [44]

3.2.2 Consent » PIPA » Children

PIPA does not specify a minimum age for consent. Under PIPA, a guardian of a minor may only act for the minor if the minor is incapable of acting.[45] Where a minor is capable of understanding what they are consenting to, the minor may consent, regardless of age. While in each instance it will depend on the individual minor, the age of consent under PIPA is usually 12 years old.

ADVICE FROM THE COMMISSIONER	Identify all your processing activities that require consent of EU data subjects. Ensure consent is freely given, specific, informed, unambiguous, explicit, and as easily revoked as given.
	Review and amend existing consent forms to ensure compatibility with GDPR requirements. Ensure processes are in place to quickly enable withdrawal of consent and create reliable records to demonstrate compliance with consent requirements.
	If the controller holds an imbalance of power over the data subject, document lawful bases for processing other than consent
	Verify individuals' ages and obtain parent or guardian consent for any processing of a minor's data. Ensure notices to children are easy to understand.

4.0 PROCESSING PERSONAL DATA WITHOUT CONSENT

4.1 Processing personal data without consent » GDPR

The GDPR permits processing of personal data without consent where it is necessary:[46]

- for executing a contract to which the data subject is a party or to take steps at the request of the data subject prior to entering into a contract;[47]
- to comply with a legal obligation to which the controller is subject;[48]
- to protect the vital interests of the data subject or another natural person;[49]
- for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;[50] or
- for the legitimate interests pursued by a controller or a third party, except where the interests or fundamental rights and freedoms of the data subject require protection of personal data, in particular where the data subject is a child.[ii]

Organizations considering processing personal data without consent should assess which of these grounds are most appropriate for their processing activities and fulfil any requirements the GDPR sets out for these conditions.[51]

Some of these bases for processing are easy to identify, such as activities that fall under performance of a contract, performance of a legal obligation, or the vital interests of the data subject. It is more difficult for organizations to assess whether their legitimate interests allow for further processing of personal information.

[ii] Note that the ground of legitimate interests is limited to the private sector, and is not available to public bodies; GDPR Article (6)(1)(f)

The recitals give examples of processing that could be necessary for the legitimate interests of a data controller, including:

- for direct marketing purposes or to prevent fraud;[52]
- to transmit personal data for internal administrative purposes, including client and employee data processing;[53]
- to ensure network and information security, including to prevent unauthorized access to electronic communications networks and to stop damage to computer and electronic computer systems;[54] or
- to report possible criminal acts or threats to public security to a competent authority.[55]

Notably, Recital 47 states that where data subjects "do not reasonably expect further processing" the data controller could not invoke legitimate interests as authority for processing. Therefore, the legitimate interests exception is limited to situations where the data subject would expect the processing to occur.

If a controller relies on legitimate interests for specific processing operations, they must explain their rationale in an information notice.[56] Individuals can object to data processing for legitimate interests.[57]

4.2 Processing personal data without consent » PIPA

PIPA also allows organizations to collect, use, and disclose personal information without consent in limited situations, such as during an investigation for breach of contract, or where the personal information is collected from a professional directory.[58]

PIPA's implied consent provisions are somewhat similar to the legitimate interests exception in the GDPR. PIPA provides for implied consent where the purpose for collection is obvious to the person providing the information; legitimate interests under the GDPR can only apply where the data subject would expect the processing to occur.[59]

An individual can cancel or change their consent by giving the organization reasonable notice, as long as doing so does not break a legal duty or promise between the organization and the individual.[60]

ADVICE FROM THE COMMISSIONER	Make sure you understand the lawful grounds for processing data that your organization plans to use. Document the decisions you make when balancing the interests of the controller and the rights of data subjects.

5.0 INDIVIDUAL RIGHTS: A COMPARISON

5.1 The right to be informed

GDPR

Under the GDPR individuals have the right to know who is collecting their data, for what purpose, how it will be stored and processed, and how to withdraw consent and make a complaint.[61] Controllers must provide information notices, to ensure transparency of processing. There is an emphasis on clear, concise notes.[62] Visualization through standardized icons is encouraged, and messaging addressed to a child should be in clear and plain language that a child can easily understand.[63]

PIPA

Under PIPA, individuals have the right to know how their personal information is collected, used, and disclosed. They also have the right to withdraw consent and make a complaint.[64]

5.2 The right to access one's personal data

GDPR

The GDPR provides individuals with the right to a copy of their personal information held by the data controller and specifies the manner in which that copy must be provided. This is explained below under the right to data portability.[65]

PIPA

Under PIPA, individuals also have the right to a copy of their personal information[66] but that copy need not be in commonly used electronic format.

5.3 The right to rectification of personal information

GDPR

Under the GDPR individuals have the right to correct their personal information. This requires controllers, upon request, to correct inaccurate or incomplete personal data.[67]

PIPA

Under PIPA, individuals also have the right to request correction of their own personal information. An organization must make the correction unless it has reasonable grounds to determine that it should not.[68] The organization must annotate the personal information with the individual's request.

The GDPR also contains rights that are not required by PIPA:

5.4 The right to erasure ("right to be forgotten")

Individuals have the right to request the deletion or removal of personal data where there is no compelling reason for its continued processing. Controllers are required to erase personal data without undue delay if the data is no longer required, if an individual withdraws consent or objects to processing, or if the processing was unlawful. A controller must take reasonable steps to communicate the erasure to other controllers who may also have that data.[69]

5.5 The right to restriction of processing

If an individual disputes the accuracy of data or objects to the processing, the individual can require the controller to restrict processing of data until the complaint is resolved.[70]

5.6 The right to data portability

Individuals have the right to a copy of their personal data from a controller. That copy must be provided in a structured, commonly used, machine-readable format. The individual may request the data be transmitted to another controller, allowing individuals to obtain, transfer, and reuse their personal data for their own purpose.[71]

5.7 The right to information about the logic involved in automated decision-making

Individuals who are subject to automated decision making, such an algorithm, have a right to meaningful information about the logic involved, such as the factors considered and how they are weighted. Individuals also have a right to know the significance and the envisaged consequences of such processing.[72]

5.8 The right not to be subject to automated decision making

The GDPR provides individuals with the right not to be subject to a decision based solely on automated processing, unless necessary for the performance of a contract between the data subject and a data controller.[73]

5.9 The right to object to data processing activities

The GDPR allows data subjects to object to data processing activities. Data subjects can object to the processing of their personal data based on legitimate interests, and the controller will be required to demonstrate compelling legitimate grounds for the processing. Individuals have the right to object at any

time to the processing of personal data including for direct marketing, profiling, and scientific or historical purposes.[74]

ADVICE FROM THE COMMISSIONER	The GDPR provides data subjects with significant additional rights that are not provided in PIPA. EU data subjects have greater privacy rights than individuals in BC.
	Implement appropriate processes and capabilities to address individual rights and requests. Update your privacy policies to reflect new requirements. Develop procedures to provide data electronically in a commonly used format and to delete personal data upon request.

6.0 MANDATORY BREACH NOTIFICATION

6.1 Mandatory breach notification » GDPR

Individuals affected by a data breach must be notified by the controller within 72 hours of discovering the breach. Breaches affecting the rights and freedoms of individuals require immediate notification, without undue delay.[75] The notification must include full details of the breach, the approximate number of individuals affected, potential consequences, and ways to mitigate any harm.[76]

6.2 Mandatory breach notification » PIPA

PIPA does not require data breach notification. However, PIPA requires that an organization protect personal information in its custody and control by making reasonable security arrangements to prevent unauthorized access, collection, use, disclosure, copying, modification or disposal, or similar risks.[77] In the event of a breach the organization may be required to notify affected individuals in order to satisfy that requirement. Our guidance document, *Privacy Breaches: Tools and Resources*,[78] is available for organizations to assess whether they have made reasonable security arrangements.

ADVICE FROM THE COMMISSIONER	BC organizations with EU data subjects should ensure that they have procedures to detect, report, and investigate a data breach as required by the GDPR.

7.0 CROSS-BORDER TRANSFERS OF PERSONAL INFORMATION

7.1 Cross-border transfers of personal information » GDPR

The GDPR permits organizations to transfer personal data outside the EU in limited circumstances including:

- to countries, territories, or sectors of a country providing an adequate level of data protection;[79]
- where standard data protection clauses or binding corporate rules apply;[80] or
- where approved codes of conduct or certification are in place.[81]

A key element of the GDPR for organizations outside of the EU is that jurisdictions with laws that are adequate in comparison to the GDPR can apply to the EU for "adequacy status." [82] Organizations in jurisdictions with adequacy status face fewer restrictions when transferring personal information outside of the EU. Canada and BC currently have adequacy status with the EU, which will continue until reviewed by the European Commission. The GDPR requires the Commission to report to the European Parliament on Canada's adequacy status by May 25, 2020.[83]

A transfer of personal data to a jurisdiction that does not have adequacy status can still occur with appropriate specific safeguards. These safeguards include standard data protection clauses, binding corporate rules, approved codes of conduct, or certification.[84]

7.2 Cross-border transfers of personal information » PIPA

PIPA does not explicitly address cross-border transfers of personal information.[iii] Section 34 requires organizations to take reasonable security measures against unauthorized access or disclosure. Under PIPA organizations can transfer personal information outside of BC but the requirement to maintain reasonable security measures continues to apply to personal information accessed, disclosed, or stored outside of BC.

ADVICE FROM THE COMMISSIONER	BC organizations can transfer personal information outside of the province but you are still required to maintain reasonable security for that personal information.

8.0 DATA GOVERNANCE OBLIGATIONS

8.1 Privacy by design » GDPR

Organizations subject to the GDPR must implement technical and organizational measures to show they have considered and included data compliance measures into their data processing activities.[85] The GDPR requires all organizations to install a number of accountability measures and show that they take data governance seriously, including privacy impact assessments,[86] audits, policy reviews, activity reports, and in some cases appointing a Data Protection Officer.[87]

[iii] This means that there are no specific restrictions to cross-border transfers under PIPA. However, all collection, use, and disclosure of personal information must be reasonable according to PIPA sections 11, 14, and 17.

8.2 Privacy by design » PIPA

PIPA requires organizations to protect and secure personal information against unauthorized use or disclosure.[88] Under PIPA, an organization must make a reasonable effort to ensure that personal information collected by or on behalf of an individual is accurate and complete, if the personal information is likely to be used by the organization to make a decision that affects the individual, or is likely to be disclosed to another organization.[89] While this requirement is less explicit than the GDPR, our office expects organizations to undertake privacy impact assessments, audits, and policy reviews to ensure compliance with PIPA.

ADVICE FROM THE COMMISSIONER	Ensure your organization builds privacy into the design, operation, and management of a system or process.

8.3 Privacy impact assessments » GDPR

Also known as data protection impact assessments, Privacy Impact Assessments (PIAs) identify and mitigate privacy risks. Data controllers are required by the GDPR to complete a PIA before initiating any processing activity with high risk of infringing on a natural person's rights and freedoms.[90]

8.4 Privacy impact assessments » PIPA

PIPA does not require private sector organizations in BC to complete PIAs; however private sector organizations are encouraged to do so. Our office is available to review your organization's PIAs, and we can also recommend improvements to your privacy management program.

ADVICE FROM THE COMMISSIONER	Make sure you complete a PIA before initiating any processing activity that has a high risk of infringing on a person's rights and freedoms.

8.5 Data protection officers » GDPR

Private sector organizations subject to the GDPR are required to appoint a data protection (DPO) officer to oversee their data processing operations where:

- the processing is carried out by a public authority or body;
- the core activities of the controller or processor consist of processing that requires regular and systematic monitoring of data subjects on a large scale;
- the core activities consist of processing special categories of data on a large scale; or
- as required by Member State law.[91]

8.6 Data protection officers » PIPA

PIPA also requires that organizations designate one or more individuals to ensure that the organization complies with PIPA. The identity and contact information of your privacy officer(s) must be publicly available.[92]

ADVICE FROM THE COMMISSIONER	At a minimum, appoint an individual responsible for privacy in your organization and publish their contact information. Assess whether or not you will fall within the mandatory DPO requirement under the GDPR.

8.7 Representatives in the EU

Controllers or processors who are not established in the EU but have EU data subjects may need to designate a representative in the EU. A controller or a processor established outside the EU must appoint a representative unless the processing is occasional, small-scale, and does not involve sensitive personal data.[93]

ADVICE FROM THE COMMISSIONER	Determine if you need a representative in the EU.

9.0 SANCTIONS

9.1 Sanctions » GDPR

Organizations that do not comply with the GDPR could face significant fines.[iv] There are two broad tiers of sanctions.

Serious infringements can result in an administrative fine up to 20 million Euros, or 4% of the total annual worldwide turnover of the business.[94] These fines apply to breaches of:

- the basic principles for processing, including conditions for consent;
- data subjects' rights;
- international transfer restrictions;
- any obligations imposed by Member State law for special cases, such as processing employee data; or
- certain orders of a supervisory authority.

[iv] Both the controller and the processor must comply with the GDPR; Article 3(1).

Lesser infringements can result in administrative fines up to 10,000,000 Euros, or 2% of total annual worldwide turnover of the business.[95] These fines apply to breach of:

- obligations of controllers and processors, including security and data breach notification obligations;
- obligations of certification bodies; or
- obligations of a monitoring body.

The GDPR also permits public interest organizations to bring class actions for data breaches on behalf of individuals who have had their rights violated.[96]

9.2 Sanctions » PIPA

Under PIPA, an individual can be liable for a fine up to $10 000 for non-compliance[97] and a person other than an individual can be liable for a fine up to $100, 000.[98]

ADVICE FROM THE COMMISSIONER	BC organizations subject to the GDPR should conduct a compliance assessment of their current policies and practices to identify gaps in relation to the GDPR.

10.0 CONCLUSION

The GDPR represents the current global standard for data protection regulation. While PIPA predates the GDPR and does not provide the same level of privacy protection, provisions such as mandatory breach notification will likely be incorporated into PIPA in the near future. Until that time, organizations can largely ensure compliance with PIPA by ensuring compliance with the GDPR, with some exceptions that are set out in the table above.

Please contact our office if you require assistance with a privacy impact assessment, implementing a privacy management program, determining whether notification of a privacy breach is appropriate, or otherwise complying with PIPA.

GLOSSARY

articles: The specific requirements of the GDPR; legally binding.

Article 29 Working Party: An advisory body made up of a representative from the data protection authority of each EU Member State, the European Data Protection Supervisor, and the European Commission.

adequacy status: A decision by the European Commission that recognizes a non-EU country as having an adequate level of privacy protection in comparison to the GDPR. Adequacy status permits transfers of information about EU citizens to companies in third countries as though those transfers were within the EU. Canada (and BC) currently has adequacy status with the GDPR.

chapter: The GDPR is organized into 11 sections, each addressing a different topic.

controller: The natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

consent: Any freely given, specific, informed, and unambiguous indication of the data subject's wishes by a statement or by a clear affirmative action signifying agreement to the processing of their personal data.

data protection impact assessment (privacy impact assessment): A structured review of a particular processing activity from a data protection compliance perspective; a tool designed to enable organizations to work out the risks that are inherent in proposed data processing activities before those activities commence.

data protection officer: An individual who is formally tasked with ensuring that an organization is aware of and complies with its data protection responsibilities.

data subject: The identified or identifiable natural person who is the subject of the personal data.

implicit consent: When an individual volunteers information for an obvious purpose and a reasonable person would think that it was appropriate for the individual to volunteer that information under those circumstances

European Commission: The EU's politically independent executive arm. It is alone responsible for drafting proposals for new European legislation, and it implements the decisions of the European Parliament and the Council of the EU.

explicit consent: An express statement of consent.

express consent: Express consent is specific permission for processing that is given either verbally or in writing.

identifiable natural person: One who can be identified, directly or indirectly, by reference to an identifier such as a name, an identification number, location data, an online identifier such as IP address, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person

implied consent: Implied consent is permission for processing that is inferred from the actions of the individual.

information notice (privacy policy): The controller must provide information to individuals about its processing of their data, unless the individual already has this information. The information must be provided in a concise, transparent, intelligible, and easily accessible way, using clear and plain language.

lead supervisory authority: The principal EU regulator responsible for enforcement of the GDPR in relation to cross border processing.

legitimate interest: Use of personal data by a data controller that is deemed necessary and would reasonably be expected by a data subject.

member state: The European Union consists of 28 member states. Member states are subject to binding laws such as the GDPR in exchange for representation within EU legislative and judicial institutions.

necessary: More than merely convenient to have; it should be integral to the provision of your product or service.

opt-out consent: When consent is presumed, but an individual can decline.

personal data: Any information relating to an identified or identifiable natural person (often referred to as a "data subject").

principle of data minimization: Meaning that processing of personal data must be limited to that which is adequate, relevant, and necessary to achieve the specified purpose.

privacy management program: A program designed to ensure that privacy is built into all initiatives, programs, or services, by design, for the responsible management of personal information.

processing: Any operation, or set of operations, which is performed on personal data or on sets of personal data, whether or not by automated means, 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

processor: Any person, public authority, or agency that processes personal data on behalf of the controller.

pseudonymization: A technique for processing personal data so that it cannot be attributed to a specific data subject without additional information.

recital: The recitals inform the interpretation of the articles, but are not legally binding.

special personal data (sensitive personal information): Revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership; data concerning health or sex life and sexual orientation; genetic data; or biometric data.

two-stage verification: A process that involves two authentication methods, performed one after the other, to verify that someone or something requesting access is who or what they declare to be.

Office of the Information & Privacy Commissioner for British Columbia

Protecting privacy. Promoting transparency.

PO Box 9038 Stn. Prov. Govt. Victoria BC V8W 9A4 | 250-387-5629 | Toll free in BC: 1-800-663-7867
info@oipc.bc.ca | oipc.bc.ca | @BCInfoPrivacy

ENDNOTES

[1] *Personal Information Protection Act,* S.B.C. 2003, c. 63 (PIPA)
[2] Regulation 2016/679 of the European Parliament and of the Council on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Advancement of Such Data, and repealing Directive 95/46/EC, 2016 O.J. L 119/1 (GDPR)
[3] GDPR Article 2
[4] GDPR Article 3(1),(2); It is not clear whether BC organizations that offer goods and services to EU businesses, as opposed to individuals, will fall under the scope of Article 3(2)(a).
[5] GDPR Article 4(2)
[6] GDPR Article 4(7)
[7] GDPR Article 4(8)
[8] GDPR Article 5(1)(a)
[9] GDPR Article 5(1)(b)
[10] GDPR Article 5(1)(c)
[11] GDPR Article 5(1)(d)
[12] GDPR Article 5(1)(e)
[13] GDPR Recital 46, Article 4(1)
[14] GDPR Recitals 10,34,35,51, Article 9(1)
[15] GDPR Article 4(5)
[16] GDPR Recital 26
[17] GDPR Recitals 28,78
[18] PIPA Section 1
[19] GDPR Article 6
[20] GDPR Article 4(11)
[21] GDPR Recitals 32
[22] GDPR Recital 171; It is unclear how this will relate to BC organizations since they were not subject to Directive 95/46/EC.
[23] GDPR Article 7(4)
[24] GDPR Article 7(3)
[25] GDPR Article 9(2)(a)
[26] GDPR Article 22
[27] GDPR Articles 45,46
[28] *Article 29 Data Protection Working Party WP29 Guidelines on Consent under Regulation 2016/679*, 2017: https://iapp.org/media/pdf/resource_center/wp29_consent-12-12-17.pdf
[29] *Ibid*
[30] GDPR Recital 43
[31] GDPR Articles 6(1)(a), 88
[32] GDPR Recitals 38, 75
[33] GDPR Articles 6(1)(f), 8
[34] GDPR Recital 58, Article 12(1)
[35] PIPA Section 6(2)(a)
[36] PIPA Section 8(3)
[37] PIPA Sections 7,8
[38] PIPA Section 9
[39] PIPA Section 12,15,18
[40] PIPA Sections 11,14,17
[41] Order P09-02, 2009, CanLII 67292 (BC IPC)
[42] PIPA Section 7(2)
[43] Order P09-01, 2009, CanLII 38705 (BC IPC)
[44] PIPA Sections 13,16,19
[45] PIPA Regulation 2
[46] GDPR Article 6(1)

[47] GDPR Article 6(1)(b)
[48] GDPR Article 6(1)(c)
[49] GDPR Article 6(1)(d)
[50] GDPR Article 6(1)(e)
[51] GDPR Article 5
[52] GDPR Recital 47
[53] GDPR Recitals 48,110; Controllers are part of the group that may have a legitimate interest, but this will be decided on a case by case basis.
[54] GDPR Recital 49
[55] GDPR Recital 50
[56] GDPR Articles 13(1)(d), 14(2)(b)
[57] GDPR Article 21
[58] PIPA Sections 12,15,18,19,20,21,22
[59] PIPA Sections 8(1)(a), 8(3)(a)
[60] PIPA Section 9
[61] GDPR Articles 12,13,14
[62] GDPR Recitals 58, 60, Article 13
[63] GDPR Recitals 38, 58, 60, Article 12(7)
[64] PIPA Sections 9,46,47
[65] GDPR Article 15
[66] PIPA Sections 23,27
[67] GDPR Article 16
[68] PIPA Sections 23,24
[69] GDPR Article 17
[70] GDPR Article 18
[71] GDPR Article 20
[72] GDPR Article 13.
[73] GDPR Article 22.
[74] GDPR Recitals 69,70, Article 21
[75] GDPR Recital 85, Articles 33(1), 34(1)
[76] GDPR Article 33(3)
[77] PIPA section 34
[78] *Privacy Breaches: Tools and Resources,* 2012; https://www.oipc.bc.ca/guidance-documents/1428
[79] GDPR Article 45(1)
[80] GDPR Articles 45(2)(b),(c),(d), 47
[81] GDPR Articles 45(2)(e),(f), 49
[82] GDPR Article 45
[83] GDPR Article 97.
[84] GDPR Recital 108, Article 46(2)
[85] GDPR Articles 5,24,25
[86] GDPR Article 35
[87] GDPR Article 37
[88] PIPA Section 34
[89] PIPA Section 33
[90] GDPR Article 35
[91] GDPR Articles 37,38,39, Recital 97, WP 243
[92] PIPA Section 4(3)
[93] GDPR Articles 27(1), 27(3)
[94] GDPR Article 83(4)
[95] GDPR Article 83(5)
[96] GDPR Articles 78, 83(9)
[97] PIPA Section 56(2)(a)
[98] PIPA Section 56(2)(b)