ICLG

The International Comparative Legal Guide to:

Data Protection 2018

5th Edition

A practical cross-border insight into data protection law

Published by Global Legal Group, with contributions from:

Affärsadvokaterna i Sverige AB
Anderson Mōri & Tomotsune
Ashurst Hong Kong
BSA Ahmad Bin Hezeem & Associates LLP
Clyde & Co
Cuatrecasas
DQ Advocates Limited
Ecija Abogados
Fırat İzgi Attorney Partnership
GANADO Advocates
GÖRG Partnerschaft von Rechtsanwälten mbB
Herbst Kinsky Rechtsanwälte GmbH
Holding Redlich
Jackson, Etti & Edu
King & Wood Mallesons
Koushos Korfiotis Papacharalambous LLC
KPMG Law Firm
Lee & Ko
Loyens & Loeff Luxembourg S.à r.l.
Loyens & Loeff N.V.
LPS L@w
Lydian
Mori Hamada & Matsumoto
Naschitz, Brandes, Amir & Co., Advocates
OLIVARES
OrionW LLC
Osler, Hoskin & Harcourt LLP
Pachiu & Associates
Pestalozzi Attorneys at law
Pillsbury Winthrop Shaw Pittman LLP
Rato, Ling, Lei & Cortés – Advogados
Rossi Asociados
Subramaniam & Associates (SNA)
Trevisan & Cuonzo Avvocati
Vaz E Dias Advogados & Associados
White & Case LLP
Wikborg Rein Advokatfirma AS

glg
global legal group

global legal group

Contributing Editors
Tim Hickman & Dr. Detlev Gabel, White & Case LLP

Sales Director
Florjan Osmani

Account Director
Oliver Smith

Sales Support Manager
Toni Hayward

Sub Editor
Oliver Chang

Senior Editors
Suzie Levy
Caroline Collingwood

Chief Executive Officer
Dror Levy

Group Consulting Editor
Alan Falach

Publisher
Rory Smith

Published by
Global Legal Group Ltd.
59 Tanner Street
London SE1 3PL, UK
Tel: +44 20 7367 0720
Fax: +44 20 7407 5255
Email: info@glgroup.co.uk
URL: www.glgroup.co.uk

GLG Cover Design
F&F Studio Design

GLG Cover Image Source
iStockphoto

Printed by
Ashford Colour Press Ltd
June 2018

ISBN 978-1-912509-15-7
ISSN 2054-3786

Strategic Partners

MIX
Paper from responsible sources
FSC® C011748

General Chapters:

Country Question and Answer Chapters:

Further copies of this book and others in the series can be ordered from the publisher. Please call +44 20 7367 0720

Canada

Adam Kardash

Patricia Kosseim

Osler, Hoskin & Harcourt LLP

1 Relevant Legislation and Competent Authorities

1.1 What is the principal data protection legislation?

Private Sector Privacy Laws in Canada

There are four private sector privacy statutes that govern the collection, use, disclosure and management of personal information in Canada: (i) the Federal *Personal Information Protection and Electronic Documents Act*, S.C. 2000, ch. 5 ("PIPEDA"); (ii) Alberta's *Personal Information Protection Act*, S.A. 2003, ch. P-6.5 ("PIPA Alberta"); (iii) British Columbia's *Personal Information Protection Act*, S.B.C. 2003, ch. 63 ("PIPA BC"); and (iv) Québec's *An Act Respecting the Protection of Personal Information in the Private Sector*, R.S.Q., ch. P-39.1 ("Québec Privacy Act"). *Collectively, these will be referred to hereinafter as the "Canadian Privacy Statutes" and will be the main focus of this chapter*.

The Federal private sector law, PIPEDA, governs the inter-provincial and international collection, use and disclosure of personal information. It applies to personal information (including employee information) held by federally regulated businesses, such as banks, airlines, railways, telecommunications companies and internet service providers, across the country.

PIPEDA also applies generally to personal information (excluding employee information) that is collected, used and disclosed by organisations in the course of a commercial activity which takes place *within* a province that does not otherwise have "substantially similar" legislation.

The private sector privacy statutes in Alberta, British Columbia and Québec (referenced above) have each been deemed "substantially similar" to PIPEDA and, as such, PIPEDA will not apply to commercial organisations operating *within* those jurisdictions, other than federally-regulated businesses which continue to be covered by PIPEDA regardless.

The health privacy statutes in Ontario, New Brunswick, Newfoundland & Labrador and Nova Scotia have also been deemed substantially similar to PIPEDA, and therefore, PIPEDA does not apply in respect of private health providers operating *within* those jurisdictions but continues to apply to other commercial activity therein. (*See the response to question 1.3 for information on health privacy legislation in Canada.*)

Public Sector Privacy Laws in Canada

Federal, provincial and territorial laws otherwise govern all public sector institutions within each of their respective jurisdictions.

1.2 Is there any other general legislation that impacts data protection?

Canada has enacted anti-spam legislation entitled *An Act to Promote the Efficiency and Adaptability of the Canadian Economy by Regulating Certain Activities that Discourage Reliance on Electronic Means of Carrying Out Commercial Activities, and to Amend the Canadian Radio-television and Telecommunications Commission Act, the Competition Act, the Personal Information Protection and Electronic Documents Act and the Telecommunications Act*, S.C. 2010, c. 23 ("Canada's anti-spam legislation" or "CASL"). (*See the response to question 9.1 for details.*)

British Columbia (*Privacy Act*, R.S.B.C. 1996, c. 373), Saskatchewan (*The Privacy Act*, R.S.S. 1978 c. Chapter P-24), Manitoba (*Privacy Act*, C.C.S.M., c. P125) and Newfoundland and Labrador (*Privacy Act*, RSNL1990, c. P-22) have also each adopted a statutory tort of invasion of privacy.

Québec civil law also provides individuals with a right to privacy under the *Civil Code of Québec*, CQLR, c. CCQ-1991 and the *Québec Charter of Human Rights and Freedoms*, CQLR, c. C-12.

1.3 Is there any sector-specific legislation that impacts data protection?

Yes. Most of the provinces in Canada have enacted health privacy legislation that applies to health information custodians in the context of providing healthcare services.

1.4 What authority(ies) are responsible for data protection?

Each Canadian jurisdiction – federally, provincially and territorially – has its own independent Information and Privacy Commissioner who reports to their respective legislature and oversees the relevant data protection laws applicable in that jurisdiction.

2 Definitions

2.1 Please provide the key definitions used in the relevant legislation:

- **"Personal Data"**

  "Personal Data" ("Personal Information") is defined very broadly under Canadian Privacy Statutes as information

about an identifiable individual. Generally, information will be deemed to be about an "identifiable individual" where it is reasonably possible for an individual to be identified through the use of that information, alone or in combination with other available information.

- **"Processing"**

  "Processing" is not expressly defined under Canadian Privacy Statutes but, in practice, would include the collection, use, modification, storage, disclosure or destruction of personal information.

- **"Controller"**

  "Controller" is not expressly defined under Canadian Privacy Statutes. Canadian Privacy Statutes refer to "organizations" more generally, which include controllers.

- **"Processor"**

  "Processor" is not defined under Canadian Privacy Statutes. Canadian Privacy Statutes refer to "organizations" more generally, which include processors.

- **"Data Subject"**

  "Data Subject" is not defined under Canadian Privacy Statutes. Canadian Privacy Statutes refer to individuals.

- **"Sensitive Personal Data"**

  "Sensitive Personal Data" is not defined under Canadian Privacy Statutes. PIPEDA provides that "any information can be sensitive depending on the context".

- **"Data Breach"**

  PIPEDA defines a "breach of security safeguards" as "the loss of, unauthorized access to or unauthorized disclosure of personal information resulting from a breach of an organization's safeguards that are referred to in clause 4.7 of Schedule 1 or from a failure to establish those safeguards".

  PIPA AB does not define "Data Breach" but requires notification to the Alberta Information and Privacy Commissioner who may in turn require notification to affected individuals "of any incident involving the loss of, or unauthorized access to, or disclosure of, the personal information where a reasonable person would consider that there exists a real risk of significant harm to an individual as a result of the loss or unauthorized access or disclosure".

- *Other key definitions – please specify (e.g., "Pseudonymous Data", "Direct Personal Data", "Indirect Personal Data")*

  There are no other key definitions in particular.

3 Territorial Scope

3.1 Do the data protection laws apply to businesses established in other jurisdictions? If so, in what circumstances would a business established in another jurisdiction be subject to those laws?

Although PIPEDA is silent with respect to its territorial reach, the Federal Court of Canada has found that PIPEDA will apply to businesses established in other jurisdictions if there is a "real and substantial connection" between the organisation's activities and Canada. With respect to websites, relevant connecting factors include: (1) where promotional efforts are being targeted; (2) the location of end-users; (3) the source of the content on the website; (4) the location of the website operator; and (5) the location of the host server.

4 Key Principles

4.1 What are the key principles that apply to the processing of personal data?

- **Transparency**

  Under the Transparency principle (also referred to as "Openness"), Canadian Privacy Statutes require organisations to document and make readily available to individuals, in a form that is generally understandable, specific information about their policies and practices relating to the management of personal information.

- **Lawful basis for processing**

  In general, Canadian Privacy Statutes require organisations to obtain consent for the collection, use and disclosure of personal information, subject to limited exceptions. In order for consent to be valid, it must be reasonable to expect that individuals would understand the nature, purpose and consequences of the collection, use or disclosure of the personal information to which they are consenting. An organisation shall not require consent, as a condition for providing a product or service, beyond that required to fulfil an explicitly specified and legitimate purpose. The form of consent (express or implied) may vary depending on the nature of the information and the reasonable expectations of the individual. Individuals may withdraw consent at any time, subject to legal or contractual restrictions and reasonable notice.

  Canadian Privacy Statutes contain a general obligation that personal information must be collected by fair and lawful means (i.e., consent must not be obtained through deception, coercion or misleading practices).

  Even with valid consent, organisations are subject to an overarching legal requirement that personal information can only be collected, used and disclosed for purposes that a reasonable person would consider appropriate in the circumstances. *See the Proportionality principle below.*

- **Purpose limitation**

  Organisations are generally required to identify the purposes for which personal information is collected at or before the time the information is collected. Organisations shall also document such purposes in accordance with the Transparency principle, *see above*.

  Personal information must not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. *See also the Data minimisation and Proportionality principles.*

- **Data minimisation**

  Canadian Privacy Statutes generally require that the collection, use and disclosure of personal information be limited (both in type and volume) to the extent to which it is necessary to fulfil the purposes identified by the organisation. Personal information shall not be retained longer than necessary to fulfil those purposes. *See the Retention principle, below.*

- **Proportionality**

  Canadian Privacy Statutes generally set out the overriding obligation that organisations may only collect, use and disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances.

  The principle of proportionality is also built into some of the other principles. For example, the safeguarding obligation imposed on organisations is proportional to the level of sensitivity,

whereby the more sensitive the information, the higher the level of protection will be required. *See Safeguarding principle below*. Similarly, the extent to which personal information shall be accurate, complete and up to date will depend upon the use being made of the information, taking into account the interests of the individual. *See Accuracy principle below.*

- **Retention**

  In keeping with the *Data Minimisation principle above*, Canadian Privacy Statutes generally require organisations to retain personal information for only as long as necessary to fulfil the purposes for which it was collected, subject to a valid legal requirement.

  Personal information that is no longer required to fulfil the identified purposes should be destroyed, erased or made anonymous.

  Organisations should develop guidelines and implement procedures for retention of personal data, including minimum and maximum retention periods and procedures governing the destruction of data.

- *Other key principles – please specify*

  Accountability – Canadian Privacy Statutes reflect the key principle of accountability. Organisations are responsible for protecting personal information under their control, including personal information that they transfer to third parties for processing, for which they must ensure a comparable level of protection through contractual or other means.

  Organisations must designate and identify an individual who is accountable for the organisation's compliance with the other privacy principles and shall implement policies and practices to give effect to those principles.

  Safeguarding – Each of the Canadian Privacy Statutes contains specific provisions relating to the safeguarding of personal information. In essence, these provisions require organisations to implement reasonable technical, physical and administrative measures to protect personal information against loss or theft, as well as unauthorised access, disclosure, copying, use, modification or destruction.

  Accuracy – Canadian Privacy Statutes contain obligations for organisations to ensure that personal information in its records is accurate, complete and up to date, particularly where the information is used to make a decision about the individual to whom the information relates or is likely to be disclosed to another organisation.

5 Individual Rights

5.1 What are the key rights that individuals have in relation to the processing of their personal data?

- **Right of access to data/copies of data**

  Under Canadian Privacy Statutes, organisations must, upon request and subject to limited exemptions, inform individuals of the existence, use and disclosure of his or her personal information, and must give them access to that information, including a listing of the third-party organisations with whom the information has been shared.

  The right of "access" does not oblige an organisation to provide copies of personal information records; rather, it requires the provision of access, which may include viewing the records at the organisation's offices. Generally, an individual's request must be sufficiently specific as to allow an organisation to identify responsive records. The organisation must respond within a prescribed time limit, or a reasonable period, as the case may be, at minimal or no cost to the individual, and must make the information available in a form that is generally understandable.

  The exemptions to the right of access vary among the statutes and need to be carefully considered. Examples of the statutory exemptions include, but are not limited to, information subject to solicitor-client or litigation privilege, confidential commercial information, information about another individual, information that relates to national security matters and information generated in a formal dispute resolution process.

- **Right to rectification of errors**

  Canadian Privacy Statutes generally require that when an individual demonstrates the inaccuracy or incompleteness of his or her personal information held by an organisation, the organisation must correct the inaccuracies and/or add a notation to the information, as appropriate.

- **Right to deletion/right to be forgotten**

  While Canadian Privacy Statutes afford individuals the right to withdraw consent and challenge the accuracy, completeness and currency of their personal data, they do not grant a specific right to require organisations to "erase" or delete their personal information *per se*.

- **Right to object to processing**

  Although Canadian Privacy Statutes do not include a specific right to object to processing, they do prohibit organisations from requiring, as a condition for providing a product or service, that individuals give consent to the collection, use or disclosure of their personal information beyond that which is required to fulfil the explicitly specified and legitimate purpose.

  Also, an individual must be able to withdraw consent at any time, subject to legal or contractual restrictions and reasonable notice. Upon receipt of any withdrawal, individuals must be informed of the implications of such withdrawal.

- **Right to restrict processing**

  See above.

- **Right to data portability**

  Although Canadian Privacy Statutes include a right of access to personal information (*see above*), they do not include a right to data portability.

- **Right to withdraw consent**

  Under Canadian Privacy Statutes, an individual must be able to withdraw consent at any time, subject to legal or contractual restrictions and reasonable notice. Individuals must be informed of the implications of such withdrawal.

- **Right to object to marketing**

  Consent is required for the collection, use or disclosure of personal information for marketing purposes. The form of consent required (opt-in or opt-out) will vary depending on the circumstances, the sensitivity of the information and the reasonable expectations of the individual. In cases where opt-out consent is appropriate, individuals must be made aware of the marketing purposes at or before the time of collection, and in a manner that is clear and understandable. Individuals must be able to easily opt-out of the practice; the opt-out must take effect immediately and be persistent; and, the information collected and used must be destroyed or effectively de-identified as soon as possible thereafter. (*See also the response to question 9.1.*)

- **Right to complain to the relevant data protection authority(ies)**

  Under Canadian Privacy Statutes, individuals have a right to make a complaint to the relevant data protection authority. Prior to this, individuals must be able to address data protection issues with the designated individual within the organisation who is accountable for the organisation's compliance. (*See Accountability principle above.*) Organisations must have easy-to-access and simple-to-use procedures in place to respond to complaints or inquiries and must take steps to effectively address complaints accordingly.

- *Other key rights – please specify*

  There are no other key rights in particular.

6 Registration Formalities and Prior Approval

6.1 Is there a legal obligation on businesses to register with or notify the data protection authority (or any other governmental body) in respect of its processing activities?

Generally, businesses do not have any legal obligation to register with or notify the relevant data protection regulatory authorities in respect of processing activities. Exceptionally, organisations that wish to use or disclose personal information without consent for statistical, or scholarly study or research, purposes must (in addition to other conditions) notify the Federal Privacy Commissioner before such use or disclosure.

(*See the response to question 15.2 for notification requirements in the event of data breaches.*)

6.2 If such registration/notification is needed, must it be specific (e.g., listing all processing activities, categories of data, etc.) or can it be general (e.g., providing a broad description of the relevant processing activities)?

This is not applicable.

6.3 On what basis are registrations/notifications made (e.g., per legal entity, per processing purpose, per data category, per system or database)?

This is not applicable.

6.4 Who must register with/notify the data protection authority (e.g., local legal entities, foreign legal entities subject to the relevant data protection legislation, representative or branch offices of foreign legal entities subject to the relevant data protection legislation)?

This is not applicable.

6.5 What information must be included in the registration/notification (e.g., details of the notifying entity, affected categories of individuals, affected categories of personal data, processing purposes)?

This is not applicable.

6.6 What are the sanctions for failure to register/notify where required?

This is not applicable.

6.7 What is the fee per registration/notification (if applicable)?

This is not applicable.

6.8 How frequently must registrations/notifications be renewed (if applicable)?

This is not applicable.

6.9 Is any prior approval required from the data protection regulator?

This is not applicable.

6.10 Can the registration/notification be completed online?

This is not applicable.

6.11 Is there a publicly available list of completed registrations/notifications?

This is not applicable.

6.12 How long does a typical registration/notification process take?

This is not applicable.

7 Appointment of a Data Protection Officer

7.1 Is the appointment of a Data Protection Officer mandatory or optional? If the appointment of a Data Protection Officer is only mandatory in some circumstances, please identify those circumstances.

PIPEDA, PIPA Alberta and PIPA BC expressly require organisations to appoint an individual who is accountable for ensuring compliance with the organisation's data protection obligations and who may, in turn, delegate some of his or her responsibilities to others. Such individuals are typically referred to as the Chief Privacy Officer or Privacy Officer, though Canadian Privacy Statutes do not prescribe any particular title.

7.2 What are the sanctions for failing to appoint a Data Protection Officer where required?

There are no specific sanctions for failure to appoint a Privacy Officer.

7.3 Is the Data Protection Officer protected from disciplinary measures, or other employment consequences, in respect to his or her role as a Data Protection Officer?

Canadian Privacy Statutes do not protect Privacy Officers against disciplinary measures as a specific function of their role. However, Privacy Officers, like other employees, enjoy some protection against retaliatory action of their employer when they, acting in good faith and based on reasonable belief, refuse to do something that will contravene the relevant data protection statute, or conversely, do something in an attempt to bring them into compliance therewith.

7.4 Can a business appoint a single Data Protection Officer to cover multiple entities?

There is no specific statutory provision that either allows or prohibits this.

7.5 Please describe any specific qualifications for the Data Protection Officer required by law.

Canadian Privacy Statutes do not set out any specific qualifications for the Privacy Officer. In a guidance document entitled *Getting Accountability Right with a Privacy Management Program* (hereinafter, "*Getting Accountability Right*"), the Federal, British Columbia and Alberta privacy regulators set out what the role of the Privacy Officer should entail, and their expectation that he or she be supported by proper training, resources and staff. Practically, a Privacy Officer would be expected to have a broad-based skill set, particularly with respect to compliance and risk management, as well as familiarity with the legal and regulatory frameworks under Canadian Privacy Statutes.

7.6 What are the responsibilities of the Data Protection Officer as required by law or best practice?

At law, a Privacy Officer is generally responsible for ensuring the organisation's compliance with the applicable privacy statute.

In *Getting Accountability Right*, the Federal, British Columbia and Alberta privacy regulatory authorities describe the role of the Privacy Officer more specifically as the individual who is accountable for structuring, designing and managing the programme, including all procedures, training, monitoring/auditing, documentation, evaluation, and follow-up. Depending on the type and size of the organisation, these Canadian privacy regulatory authorities expect the Privacy Officer to, among other things: establish and implement programme controls, in coordination with other appropriate persons responsible for related functions within the organisation; be responsible for the ongoing assessment and revision of programme controls; represent the organisation in the event of a complaint investigation by a Privacy Commissioner's office; and most critically, advocate privacy protection within the organisation itself.

7.7 Must the appointment of a Data Protection Officer be registered/notified to the relevant data protection authority(ies)?

There is no requirement to register or notify the Data Protection Officer with the relevant data protection authorities.

7.8 Must the Data Protection Officer be named in a public-facing privacy notice or equivalent document?

Organisations must be open about, and make available in a form that is generally understandable, the contact information of the person who is accountable for the organisation's policies and practices and to whom complaints or inquiries can be made. Canadian privacy regulatory authorities expect the Privacy Officer's contact information to be included in a public-facing privacy policy.

8 Appointment of Processors

8.1 If a business appoints a processor to process personal data on its behalf, must the business enter into any form of agreement with that processor?

Yes, under PIPEDA, an organisation is required to "use contractual or other means to provide a comparable level of protection while the information is being processed by a third party". The failure to have appropriate confidentiality agreements in place with third-party contractors has been found to be a breach of the accountability principle.

8.2 If it is necessary to enter into an agreement, what are the formalities of that agreement (e.g., in writing, signed, etc.) and what issues must it address (e.g., only processing personal data in accordance with relevant instructions, keeping personal data secure, etc.)?

In the private sector context, Canadian Privacy Statutes do not specify the requirements to be included in agreements with third-party processors. However, some privacy laws, and their accompanying regulations, in the health sector for instance, more expressly set out the terms and conditions to be included in written agreements between institutions and information managers. (*See, for example, section 66 of Alberta's Health Information Act, R.S.A. 2000, c. H-5, and accompanying Regulation 70/2001.*)

9 Marketing

9.1 Please describe any legislative restrictions on the sending of electronic direct marketing. (E.g., for marketing by email or SMS, is there a requirement to obtain prior opt-in consent of the recipient?)

The sending of email and SMS text messages is subject to both the requirements under Canadian Privacy Statutes and Canada's anti-spam legislation ("CASL"). In general, under CASL, it is a violation to send, or cause or permit to be sent, a commercial electronic message (defined broadly to include text, sound, voice or image messages) to an electronic address unless the recipient has provided express or implied consent (as defined in the Act) and the message complies with the prescribed form and content requirements, including an unsubscribe mechanism.

9.2 Please describe any legislative restrictions on the sending of marketing via other means (e.g., for marketing by telephone, a national opt-out register must be checked in advance; for marketing by post, there are no consent or opt-out requirements, etc.)

Telephone marketing in Canada is subject to the requirements of Canadian Privacy Statutes as well as the Canadian Radio-Television and Telecommunications Commission's ("CRTC") Unsolicited Telecommunications Rules. These rules include specific requirements related to the National Do-Not-Call List ("National DNCL"), telemarketing and the use of automatic dialling-announcing devices.

Under Canada's Do-Not-Call List Rules ("DNCL Rules"), an individual may register their telephone or fax number on the National DNCL to indicate that they do not wish to receive unsolicited telemarketing communications. In general, organisations are prohibited from placing unsolicited telemarketing calls (telephone or fax) to numbers registered on the National DNCL unless express consent has been obtained directly from the individual in the manner prescribed under the DNCL Rules. Under the CRTC Telemarketing Rules, an organisation must maintain its own internal Do-Not-Call List and must not initiate telemarketing telecommunications to an individual on its own list.

Postal marketing communications are not specifically regulated, but must comply with the requirements of Canadian Privacy Statutes.

9.3 Do the restrictions noted above apply to marketing sent from other jurisdictions?

Yes, they do apply.

9.4 Is/are the relevant data protection authority(ies) active in enforcement of breaches of marketing restrictions?

Yes. The Canadian privacy regulatory authorities have issued multiple reports of findings related to secondary marketing practices. The CRTC is also active in enforcing the Unsolicited Telecommunications Rules.

Canada's anti-spam legislation ("CASL") came into force on July 1, 2014. The CRTC has been actively enforcing CASL and has completed dozens of investigations over the past three years.

9.5 Is it lawful to purchase marketing lists from third parties? If so, are there any best practice recommendations on using such lists?

It is only lawful if the individuals on the list were clearly and accurately informed at the point of collection about how their addresses would be used and if they consented to having their email addresses collected and used for marketing purposes. In addition, they must be able to opt-out of receiving messages at any time in the future.

9.6 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?

Under Canadian Privacy Statutes, there are no specific penalties related to the unlawful sending of marketing communications. However, organisations may be subject to a complaint and investigation. In Alberta, British Columbia and Québec, an investigation may be elevated to a formal inquiry resulting in an order. Failure to comply with an order can result in fines of up to $100,000 in Alberta and British Columbia. In Alberta and Québec, organisations can also be subject to fines for failure to comply with the relevant requirements of the Acts of up to $100,000 in Alberta and $10,000 in Québec for a first offence and $20,000 for a subsequent offence.

The CRTC has the legislative authority under the *Telecommunications Act* to impose administrative monetary penalties for violation of the Unsolicited Telecommunications Rules. The maximum administrative monetary penalty for each violation of the Unsolicited Telecommunications Rules is $15,000 for a corporation. A violation that continues for more than one day constitutes a separate violation for each day that it is continued. In addition, a person that contravenes any prohibition or requirement of the Commission related to the Unsolicited Telecommunications Rules may be guilty of an offence punishable on summary conviction and liable, in the case of a corporation, to a fine not exceeding $100,000 for a first offence or $250,000 for a subsequent offence. There is also a limited private right of action that allows a person to sue for damages that result from any act or omission that is contrary to the *Telecommunications Act* or a decision or regulations.

The CRTC is also the agency primarily responsible for regulatory enforcement of CASL's commercial electronic message provisions. CASL permits the CRTC to impose administrative monetary penalties of up to $1 million per violation for individuals and $10 million for businesses. CASL outlines a range of factors to be considered in assessing the penalty amount, including the nature and scope of the violation. CASL also sets forth a private right of action permitting individuals to bring a civil action for alleged violations of CASL ($200 for each contravention up to a maximum of $1 million each day for a violation of the provisions addressing unsolicited electronic messages).

10 Cookies

10.1 Please describe any legislative restrictions on the use of cookies (or similar technologies).

There are no specific restrictions with respect to cookies under Canadian Privacy Statutes. As with other forms of collection, use and disclosure of personal information in the course of commercial activities, cookies are subject to the general requirements of Canadian Privacy Statutes.

Under Canadian Privacy Statutes, implied consent can be relied upon for the collection and use of personal information through cookies to the extent that the personal information involved is non-sensitive in nature and that it accords with the reasonable expectations of individuals.

The Privacy Commissioner of Canada's regulatory guidance on *Online Behavioural Advertising* affirmed that implied (or opt-out) consent is reasonable for the purposes of online behavioural advertising provided that:

- individuals are made aware of the purposes for the practice in a manner that is clear and understandable;
- individuals are informed of these purposes at or before the time of collection and provided with information about the various parties involved in online behavioural advertising;
- individuals are able to easily opt-out of the practice at or before the time the information is collected;
- the opt-out takes effect immediately and is persistent;
- the information collected and used is limited, to the extent practicable, to non-sensitive information; and
- information collected and used is destroyed as soon as possible or effectively de-identified.

If, however, the personal information collected and used is sensitive in nature, express consent is required.

10.2 Do the applicable restrictions (if any) distinguish between different types of cookies? If so, what are the relevant factors?

Although there are no explicit legislative restrictions with respect to cookies specifically, the Office of the Privacy Commissioner of Canada ("OPC") has restricted the following uses:

The first is in respect of zombie cookies, supercookies, third-party cookies that appear to be first-party cookies, device fingerprinting and other techniques that cannot be controlled by individuals. Where a tracking technique offers no option for user control, and therefore no ability for an individual to consent or withdraw consent to the collection of their personal information for online behavioural advertising purposes, the OPC's position is that that such tracking should not be undertaken because it cannot be done in compliance with PIPEDA.

Secondly, given the practical obstacles to obtaining meaningful consent from children, the OPC's position is that organisations should avoid knowingly tracking children and tracking on websites aimed at children. The OPC takes the view 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. Youth between 13 years and the applicable age of majority can give meaningful consent, provided the organisation's consent process reasonably takes into account their level of maturity and is adapted accordingly.

10.3 To date, has/have the relevant data protection authority(ies) taken any enforcement action in relation to cookies?

Yes. The OPC has issued several reports of findings in cases involving cookies in the context of online behavioural advertising. As examples, one case involved sensitive health information (PIPEDA Report of Findings #2014-001), and the other involved a website aimed at children (PIPEDA Report of Findings #2014-011).

10.4 What are the maximum penalties for breaches of applicable cookie restrictions?

Under Canadian Privacy Statutes, there are no specific penalties related to cookie restrictions. However, organisations may be subject to a complaint and investigation under Canadian Privacy Statutes. In Alberta and British Columbia, an investigation may be elevated to a formal inquiry resulting in an order. Failure to comply with an order can result in fines of up to $100,000. In Alberta and Québec, organisations can also be subject to fines for failure to comply with the relevant requirements of the Acts of up to $100,000 in Alberta and $10,000 in Québec for a first offence and $20,000 for a subsequent offence.

11 Restrictions on International Data Transfers

11.1 Please describe any restrictions on the transfer of personal data to other jurisdictions.

Under Canadian Privacy Statutes governing the private sector, organisations are responsible for personal information in their custody or control, including personal information transferred to third parties for processing. In general, Canadian Privacy Statutes permit the non-consensual transfer of personal information to third-party processors outside Canada, provided the transferring organisation uses contractual or other means to provide a comparable level of protection while the information is being processed by the foreign processor.

In Alberta, more specifically, if an organisation uses a service provider outside Canada to collect, use, disclose or store personal information, the organisation must specify, in its privacy policies and practices, the foreign jurisdictions in which the collection, use, disclosure or storage is taking place, and the purposes for which the foreign service provider has been authorised to collect, use or disclose personal information on its behalf.

11.2 Please describe the mechanisms companies typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions (e.g., consent of the data subject, performance of a contract with the data subject, approved contractual clauses, compliance with legal obligations, etc.).

Typically, companies enter into an agreement when transferring data outside of Canada for processing purposes to ensure that the data transferred is afforded a comparable level of protection to that under Canadian Privacy Statutes. Depending on the size and the context of the data transfer arrangement in question, there are a number of measures that companies take to establish an appropriate vendor management framework, including: (i) due diligence, in particular with respect to security safeguards; (ii) contractual arrangements setting out requisite controls and conditions; (iii) appropriate notice to employees or consumers; and (iv) appropriate monitoring of the service provider arrangement. While consent *per se* is not required, notification is.

11.3 Do transfers of personal data to other jurisdictions require registration/notification or prior approval from the relevant data protection authority(ies)? Please describe which types of transfers require approval or notification, what those steps involve, and how long they typically take.

Transfers of personal data to other jurisdictions do not require registration/notification or prior approval from the relevant data protection authorities.

12 Whistle-blower Hotlines

12.1 What is the permitted scope of corporate whistle-blower hotlines (e.g., restrictions on the types of issues that may be reported, the persons who may submit a report, the persons whom a report may concern, etc.)?

Under Canadian Privacy Statutes, a whistle-blower who has reasonable grounds to believe that a provision of the relevant statute has been, or will be, contravened may notify the data protection authority and request that their identify be kept confidential. The data protection authority shall keep confidential the person's identity and the information he or she relayed, accordingly.

The statutes further prohibit employers from taking retaliatory action against an employee who, acting in good faith and on the basis of reasonable belief, disclosed such information to the data protection authority. Any employer who knowingly contravenes this prohibition is guilty of an offence and may be subject to a fine.

12.2 Is anonymous reporting prohibited, or strongly discouraged, or generally permitted? If it is prohibited or discouraged, how do companies typically address this issue?

Anonymous reporting is not prohibited or discouraged under Canadian Privacy Statutes. As a matter of practice, anonymous

reporting of facts that are credible and can be independently verified may proceed as a Commissioner-initiated complaint if there are reasonable grounds to believe that an investigation is warranted.

13 CCTV

13.1 Does the use of CCTV require separate registration/notification or prior approval from the relevant data protection authority(ies), and/or any specific form of public notice (e.g., a high-visibility sign)?

The use of CCTV does not require separate registration/notification or prior approval from the relevant data protection authorities. However, as a best practice in some jurisdictions, and as a matter of policy in others, organisations must conduct a privacy impact assessment and seek input from the relevant data protection authority before introducing the use of CCTV.

Appropriate and clear notice should be provided to individuals prior to the collection of personal information through video surveillance. This notice should include the purposes of the video surveillance and contact information in case the individual has questions or wishes to request access to their images.

13.2 Are there limits on the purposes for which CCTV data may be used?

The use of CCTV must only be for purposes that a reasonable person would consider to be appropriate in the circumstances. For instance, the use of CCTV to ensure the protection of company assets that have come under threat of being damaged or stolen, or the safety of customers in situations that have proven to be demonstrably dangerous may be considered reasonable. On the other hand, using CCTV to generally monitor employee performance in the absence of any prior concerns having been raised or any suspected wrongdoing may not be.

14 Employee Monitoring

14.1 What types of employee monitoring are permitted (if any), and in what circumstances?

Employee monitoring would be permissible (both in the workplace and otherwise), provided that it is conducted in conformity with the principles under Canadian Privacy Statutes.

In particular, the monitoring must be conducted for a purpose consistent with what a reasonable person would consider appropriate in the circumstances. Canadian privacy regulatory authorities generally use a four-part test to assist in determining the reasonableness of employee monitoring:

- Is the surveillance demonstrably necessary to meet a specific need?
- Is the measure likely to be effective in meeting that need?
- Is the loss of privacy proportional to the benefit gained?
- Is there a less privacy-invasive way that the employer could achieve the same end?

14.2 Is consent or notice required? Describe how employers typically obtain consent or provide notice.

Canadian privacy statutes governing the private sector generally allow for the collection, use and disclosure of employee personal information without consent if it is solely for the purposes reasonably required to establish, manage or terminate an employment relationship between the organisation and that individual.

While the statutes allow for the collection of personal information without consent, within the bounds of reasonableness, they nonetheless require the employer to be transparent about it; accordingly, organisations must notify employees that it is occurring, and explain the purpose(s) for the collection (such as employee safety).

Employers typically provide notice about video surveillance or monitoring upon entry to the workplace area under surveillance or upon use of the technology being monitored. Employers also implement video surveillance and monitoring policies and reference such activities in relevant privacy statements.

14.3 To what extent do works councils/trade unions/employee representatives need to be notified or consulted?

There is no express requirement to notify trade unions regarding the use of employee monitoring under Canadian Privacy Statutes.

15 Data Security and Data Breach

15.1 Is there a general obligation to ensure the security of personal data? If so, which entities are responsible for ensuring that data are kept secure (e.g., controllers, processors, etc.)?

Canadian Privacy Statutes contain specific provisions relating to the safeguarding of personal information. In essence, these provisions require organisations to implement reasonable technical, physical and administrative measures to protect personal information against loss or theft, as well as unauthorised access, disclosure, copying, use, modification or destruction. The security safeguards must be appropriate to the sensitivity of the information, such that, the more sensitive the information, the higher the level of protection that will be required.

An organisation is responsible for protecting personal information in its possession or custody, including information that has been transferred to a third party for processing. They must ensure a comparable level of protection through contractual or other means.

15.2 Is there a legal requirement to report data breaches to the relevant data protection authority(ies)? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expects voluntary breach reporting.

The Federal private sector privacy law, PIPEDA, was amended in 2015 to include new breach notification requirements that will come into force November 1, 2018. Once these provisions are in force, PIPEDA will require organisations to report to the Privacy Commissioner any breach of security safeguards involving personal 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. The report must be made in prescribed form and manner and provided as soon as feasible after the organisation determines that the breach has occurred. Reports to the Commissioner must include the following:

a. a description of the circumstances of the breach and, if known, the cause;

b. the day on which, or the period during which, the breach occurred or, if neither is known, the approximate period;

c. a description of the personal information that is the subject of the breach to the extent that the information is known;

d. the number of individuals affected by the breach or, if unknown, the approximate number;

e. a description of the steps that the organisation has taken to reduce the risk of harm to affected individuals that could result from the breach or to mitigate that harm;

f. a description of the steps that the organisation has taken or intends to take to notify affected individuals of the breach; and

g. the name and contact information of a person who can answer, on behalf of the organisation, the Commissioner's questions about the breach.

Moreover, the new breach provisions in PIPEDA will require organisations to keep records, in prescribed form, of every breach of security safeguards involving personal information under its control, and to provide the Commissioner with a copy of such records on request.

Under PIPA Alberta, an organisation is required to provide notice to the Commissioner without unreasonable delay of a breach where there is a real risk of significant harm to individuals. Notice to the Commissioner must be in writing and include similar details as those that will be required under PIPEDA (above).

15.3 Is there a legal requirement to report data breaches to affected data subjects? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expects voluntary breach reporting.

As of November 1, 2018, PIPEDA's breach notification provisions will require an organisation to notify affected individuals of a breach of security safeguards if it is reasonable in the circumstances to believe that the breach creates a real risk of significant harm to the individual. The notification must be given as soon as feasible after the organisation determines that the breach has occurred. It must be conspicuous and given directly to the individual in the manner prescribed by the regulations. Indirect notification is also permissible in circumstances where direct notification is likely to cause further harm to the affected individual or undue hardship for the organisation, or where the organisation does not have contact information for the affected individual.

The contents of the notification to individuals will have to include:

a. a description of the circumstances of the breach;

b. the day on which, or period during which, the breach occurred or, if neither is known, the approximate period;

c. a description of the personal information that is the subject of the breach to the extent that the information is known;

d. a description of the steps that the organisation has taken to reduce the risk of harm that could result from the breach;

e. a description of the steps that affected individuals could take to reduce the risk of harm that could result from the breach or to mitigate that harm; and

f. contact information that the affected individual can use to obtain further information about the breach.

Under PIPEDA, when notice is given to individuals, it must also be given to any other organisation or government institution if the notifying organisation believes that the other organisation or the government institution may be able to reduce the risk of harm or mitigate that harm.

Under PIPA Alberta, the Commissioner, once notified, may subsequently require organisations to notify affected individuals directly of the loss or unauthorised disclosure, unless the Commissioner determines that direct notification would be unreasonable in the circumstances. Such notification must include certain elements which are similar to those that will be required under PIPEDA (above).

While other data protection statutes do not contain any express data breach notification requirements, Commissioners' findings and other guidance documents suggest that a duty to notify affected individuals is an implicit part of the general safeguarding requirements in circumstances where material harm is reasonably foreseeable, and such notification would serve to protect personal information from further unauthorised access, use or disclosure.

15.4 What are the maximum penalties for data security breaches?

Under PIPEDA, failure to comply with the breach notification provisions will (as of November 1, 2018) be an offence under the Act punishable on summary conviction liable to a fine not exceeding $10,000, or as an indictable offence liable to a fine not exceeding $100,000.

Under PIPA Alberta, a failure to notify the Commissioner in the event of a breach is an offence. A person who commits an offence is liable, in the case of an individual, to a fine not exceeding $10,000, and in the case of a person other than an individual, to a fine not exceeding $100,000.

16 Enforcement and Sanctions

16.1 Describe the enforcement powers of the data protection authority(ies).

Powers of Investigation

Under PIPEDA, the Federal Privacy Commissioner shall investigate a complaint made by an individual, subject to a discretion to decline or discontinue complaints in certain circumstances.

The Federal Privacy Commissioner can also initiate an investigation based on reasonable grounds to believe that a matter warrants it.

In the course of an investigation, the Commissioner has substantial powers, including the power to summon witnesses to give oral or written evidence, inspect documents and/or compel the production thereof, and inspect premises other than a dwelling house.

Under PIPA Alberta and PIPA BC, the Commissioners have similar powers of investigation. However, where a matter is not otherwise resolved, an investigation may be elevated to a formal inquiry.

Powers of Enforcement

Upon concluding an investigation under PIPEDA, the Privacy Commissioner issues a report of findings and, if applicable, recommendations for compliance. Although the report is non-binding in nature, it may be made public at the discretion of the Privacy Commissioner if it is in the public interest.

The complainant or the Commissioner, with the individual's consent, may apply to the Federal Court for a *de novo* hearing. The Court has broad remedial powers to order correction of the organisation's practices and award damages to the complainant, including damages for any "humiliation" suffered.

The OPC and the organisation may agree to enter into a voluntary compliance agreement whereby the organisation undertakes to comply with the recommendations made and bring itself into compliance with PIPEDA.

When a compliance agreement is entered into, the Commissioner shall not apply to the Court for a hearing or shall suspend any pending court application, unless or until there is breach of the agreement. If an organisation fails to live up to its commitments in a compliance agreement, the OPC could, after notifying the organisation, apply to the Court for an order requiring the organisation to comply with the terms of the agreement.

In Alberta and British Columbia, an inquiry may result in an enforceable order. Organisations are required to comply with the order within a prescribed time period, unless they apply for judicial review. In Alberta, the order may be filed with the Court and becomes enforceable as a judgment. Once an order is final, an affected individual has a cause of action against the organisation for damages for loss or injury that the individual has suffered as a result of the breach.

Similarly, in Québec, an order must be obeyed within a prescribed time period. An individual may appeal to the judge of the Court of Québec on questions of law or jurisdiction with respect to a final decision.

Audits

The OPC and the OIPC BC have the express authority to audit the personal information practices of an organisation upon reasonable grounds that the organisation is contravening the Act. The results of the audit are made public.

Offences / Criminal Sanctions

In Québec, Alberta and British Columbia, there are certain statutory provisions which, if violated, could constitute an offence and result in fines of up to $10,000 for a first offence and $20,000 for a subsequent offence in Québec, and $100,000 for an offence in Alberta and British Columbia. This includes the offence of failing to comply with an order made by the Commissioner.

Under PIPEDA, there are more limited statutory provisions, the contravention of which may result in criminal sanctions. For example, any person who knowingly destroys personal information that is the subject of an access to personal information request, retaliates against a whistle-blowing employee, obstructs the Commissioner in the course of a complaint investigation, uses deception or coercion to collect personal information in contravention of the Act, or (as of November 1, 2018) fails to notify in the event of a breach, is guilty of an offence and liable to a fine of $10,000 for an offence punishable on summary conviction or $100,000 for an indictable offence.

Data-Sharing Arrangements

The Privacy Commissioner of Canada has the express authority under PIPEDA to enter into data-sharing arrangements with provincial or foreign counterparts, as considered appropriate, to coordinate their Office's activities, (including investigations) and ensure that personal information is protected in as consistent a manner as possible.

16.2 Does the data protection authority have the power to issue a ban on a particular processing activity? If so, does such a ban require a court order?

To the extent that data protection authorities have the power to issue binding orders (*see above*), they can ban a particular processing activity or apply to the Court for an enforceable order to that effect.

16.3 Describe the data protection authority's approach to exercising those powers, with examples of recent cases.

Canada has one of the most active privacy regulatory enforcement arenas in the world. The OPC and the provincial privacy regulatory authorities in the provinces of Alberta and British Columbia have been actively focused on early resolving individual complaints wherever possible, in order to redirect limited resources to the investigation of novel, precedent-setting complaints that raise large, systemic issues particularly in the online world (including complaints against companies such as Facebook and Google).

There has also been an increasing trend of Canadian privacy regulatory authorities initiating investigations of their own accord. The OPC, in particular, is adopting a deliberate strategy of proactive enforcement through formal, Commissioner-initiated investigations, as well as active participation in the less formal, online privacy sweeps of the Global Privacy Enforcement Network ("GPEN").

The OPC is also collaborating more frequently with its national and international counterparts, to conduct joint investigations in accordance with formal written arrangements (e.g., Ashley Madison and WhatsApp).

Canadian privacy regulators actively pursue softer compliance tools as well, such as guideline development, public education and research on a range of emerging privacy issues – both individually and jointly – to encourage compliance up front before problems arise.

16.4 Does the data protection authority ever exercise its powers against companies established in other jurisdictions? If so, how is this enforced?

Although PIPEDA is silent with respect to its territorial reach, the Federal Court of Canada has found that PIPEDA will apply to businesses established in other jurisdictions if there is a "real and substantial connection" between the organisation's activities and Canada. For instance, with respect to websites, the relevant connecting factors include: (1) where promotional efforts are being targeted; (2) the location of end-users; (3) the source of the content on the website; (4) the location of the website operator; and (5) the location of the host server.

17 E-discovery / Disclosure to Foreign Law Enforcement Agencies

17.1 How do companies typically respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?

Although the language varies across the statutes, under Canadian Privacy Statutes, there is generally an exception to the consent requirement when disclosing information (i) to comply with the rules of court relating to the production of records, and (ii) where required by law.

When disclosing personal information in either of these contexts, the remaining requirements under Canadian Privacy Statutes still apply. As such, organisations must only disclose the personal information in the manner and to the extent to which a reasonable person would consider appropriate in the circumstances, must limit the amount of personal information that is disclosed to that which is reasonably necessary in the circumstances, and must appropriately safeguard the transmission of personal information.

The OPC also expects organisations to be open and transparent when transferring data across borders, in particular by openly notifying individuals that personal information transferred to another jurisdiction becomes subject to foreign laws and may be accessed by the courts, law enforcement and national security authorities in those jurisdictions.

17.2 What guidance has/have the data protection authority(ies) issued?

The OPC has released a guidance document entitled *Guidelines for Processing Personal Data Across Borders* which addresses lawful access by foreign authorities.

The OPC has also released a guidance document entitled *PIPEDA and Your Practice: A Privacy Handbook for Lawyers* which addresses privacy issues associated with e-discovery.

18 Trends and Developments

18.1 What enforcement trends have emerged during the previous 12 months? Describe any relevant case law.

See above a description of the more proactive enforcement trends that have emerged during recent years, including the previous 12 months.

In terms of relevant case law, courts continue to refine the contours of common law privacy torts, including the tort of invasion of privacy and the tort of publication of embarrassing private facts.

Also, the Supreme Court of Canada has over the past year rendered two important decisions: one on the validity of the forum selection clause used by Facebook in its terms of use (*Douez v. Facebook Inc., 2017 SCC 33*); and the other on the validity of a British Columbia court-ordered injunction against Google to globally de-index websites of a certain distributor who was continuing to act unlawfully (*Google Inc. v. Equustek Solutions Inc., 2017 SCC 34*).

This coming year, in a case called *R. v. Jarvis*, the Supreme Court of Canada will be asked to define the concept of reasonable expectation of privacy in public places for the purpose of enforcing voyeurism provisions of the Criminal Code of Canada.

18.2 What "hot topics" are currently a focus for the data protection regulator?

Canada's Federal Privacy regulator, the OPC, has established four strategic privacy priorities to guide the Office's discretionary work through 2020: economics of personal information; government surveillance; reputation and privacy; and the body as information.

The Office is currently focused on implementing its recommendations for enhanced consent under PIPEDA, including by finalising its online consent guidance this year, among other related guidance documents it intends to publish both for organisations and individuals in the short to medium term, including on de-identification.

The OPC continues to focus on national security reforms in Canada and the interplay with data protection. The Office also intends to finalise its policy position on the right to be forgotten in Canada and continues to shift its focus towards more proactive enforcement of broad systemic issues in collaboration with its national and international counterparts.

Canadian privacy regulators are increasingly interested in the role that ethics should play in the effective governance of big data, analytics and artificial intelligence initiatives. There is also an active interest on the part of Canadian regulators to pursue the growing intersection between data protection, competition and consumer protection law, and a recognition of the corresponding need for increased collaboration between them.

The CRTC continues to actively enforce the commercial electronic message provisions in CASL. The CRTC has entered into five undertakings regarding potential CASL violations that included payments to the CRTC ranging from $10,000 to $200,000, and has made three compliance and enforcement decisions with administrative monetary penalties ranging from $15,000 to $200,000.

Adam Kardash
Osler, Hoskin & Harcourt LLP
100 King Street West
1 First Canadian Place
Suite 6200, P.O. Box 50
Toronto ON M5X 1B8
Canada

Tel: +1 416 862 4703
Email: akardash@osler.com
URL: www.osler.com

Adam is an acknowledged Canadian legal industry leader in privacy and data management; he co-leads Osler's national Privacy and Data Management Group. Adam has been lead counsel on many of the most significant privacy matters in Canada. He advises Fortune 500 clients in their business-critical data protection issues, compliance initiatives and data governance. He regularly represents clients on regulatory investigations and security breaches.

Adam is Special Counsel to the Interactive Advertising Bureau of Canada and Counsel to the Digital Advertising Alliance of Canada. He has extensive experience in the privacy law area and regularly advises Chief Privacy Officers, in-house counsel and compliance professionals in the private, health, public and not-for-profit sectors on managing security incidents, privacy regulatory investigations, anti-spam law compliance, privacy and security reviews/audits, privacy policies, practices and procedures, privacy compliance initiatives, and service provider arrangements involving personal information, including trans-border data flows.

For further information, please visit https://www.osler.com/en/team/adam-kardash.

Patricia Kosseim
Osler, Hoskin & Harcourt LLP
Suite 1900
340 Albert Street
Ottawa ON K1R 7Y6
Canada

Tel: +1 613 787 1008
Email: pkosseim@osler.com
URL: www.osler.com

Patricia is Counsel in Osler's Privacy and Data Management Group and Co-Leader of Osler's AccessPrivacy© platform. Patricia is a national leading expert in privacy and access law, having served over a decade as Senior General Counsel at the Office of the Privacy Commissioner of Canada (OPC). There she: provided strategic legal and policy advice on complex privacy issues; advised Parliament on privacy implications of legislative bills; led research initiatives on emerging information technologies; and advanced privacy law in major litigation cases before the courts, including the Supreme Court of Canada.

Previously, Patricia worked at Genome Canada and the Canadian Institutes of Health Research, where she developed and led national strategies for addressing legal, ethical and social implications of science and technology. Patricia began her career in Montreal practising in the areas of health law, privacy law, civil litigation, and labour and employment with another leading national law firm. She has published and spoken extensively on matters of privacy law, health law and ethics.

For further information, please visit https://www.osler.com/en/team/patricia-kosseim.

OSLER
Osler, Hoskin
& Harcourt LLP

Osler is a leading business law firm advising Canadian and international clients from offices across Canada and in New York. With well over 400 lawyers, the firm is recognised for the breadth and depth of its practice and is consistently ranked as one of Canada's top firms in national and international surveys. Osler has the largest team of practitioners who focus exclusively on privacy and data management in Canada, providing expert legal advice on increasingly complex issues.

Osler's AccessPrivacy© provides an integrated suite of innovative information solutions, consulting services and thought leadership. The AccessPrivacy© platform helps organisations in the public, private and not-for-profit sectors navigate the complex regulatory environment and develop a strategic approach to privacy and information management, supported by sound policies and practices.

Other titles in the ICLG series include:

- Alternative Investment Funds
- Anti-Money Laundering
- Aviation Law
- Business Crime
- Cartels & Leniency
- Class & Group Actions
- Competition Litigation
- Construction & Engineering Law
- Copyright
- Corporate Governance
- Corporate Immigration
- Corporate Investigations
- Corporate Recovery & Insolvency
- Corporate Tax
- Cybersecurity
- Employment & Labour Law
- Enforcement of Foreign Judgments
- Environment & Climate Change Law
- Family Law
- Fintech
- Franchise
- Gambling
- Insurance & Reinsurance
- International Arbitration
- Investor-State Arbitration
- Lending & Secured Finance
- Litigation & Dispute Resolution
- Merger Control
- Mergers & Acquisitions
- Mining Law
- Oil & Gas Regulation
- Outsourcing
- Patents
- Pharmaceutical Advertising
- Private Client
- Private Equity
- Product Liability
- Project Finance
- Public Investment Funds
- Public Procurement
- Real Estate
- Securitisation
- Shipping Law
- Telecoms, Media & Internet
- Trade Marks
- Vertical Agreements and Dominant Firms

glg global legal group

59 Tanner Street, London SE1 3PL, United Kingdom
Tel: +44 20 7367 0720 / Fax: +44 20 7407 5255
Email: info@glgroup.co.uk

www.iclg.com