International
Comparative
Legal Guides

Data Protection 2021

A practical cross-border insight into data protection law

Eighth Edition

Featuring contributions from:

Anderson Mōri & Tomotsune
Arthur Cox LLP
Chandler MHM Limited
CO:PLAY Advokatpartnerselskab
D'LIGHT Law Group
DQ Advocates Limited
Drew & Napier LLC
FABIAN PRIVACY LEGAL GmbH
Foucaud Tchekhoff Pochet et Associés (FTPA)
H & A Partners
in association with Anderson Mōri & Tomotsune
Hajji & Associés
Hammad and Al-Mehdar Law Firm
Homburger
Iriarte & Asociados
Khaitan & Co LLP
King & Wood Mallesons
Klochenko & Partners Attorneys at Law
Koushos Korfiotis Papacharalambous LLC
Law Firm Pirc Musar & Lemut Strle Ltd
Lee and Li, Attorneys At Law
Leśniewski Borkiewicz & Partners
LPS L@W
LYDIAN
McMillan LLP
MinterEllison
Mori Hamada & Matsumoto
Naschitz, Brandes, Amir & Co., Advocates
Nikolinakos & Partners Law Firm
OLIVARES
Pinheiro Neto Advogados
PLANIT // LEGAL
S. U. Khan Associates Corporate & Legal Consultants
SEOR Law Firm
White & Case LLP
Wikborg Rein Advokatfirma AS

ICLG.com

ISBN 978-1-83918-127-6
ISSN 2054-3786

Published by
global legal group
59 Tanner Street
London SE1 3PL
United Kingdom
+44 207 367 0720
info@glgroup.co.uk
www.iclg.com

Publisher
James Strode

Production Editor
Jane Simmons

Senior Editor
Sam Friend

Head of Production
Suzie Levy

Chief Media Officer
Fraser Allan

CEO
Jason Byles

Printed by
Ashford Colour Press Ltd.

Cover image
www.istockphoto.com

Strategic Partners

International Comparative Legal Guides

Data Protection 2021

Eighth Edition

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

©2021 Global Legal Group Limited.
All rights reserved. Unauthorised reproduction by any means, digital or analogue, in whole or in part, is strictly forbidden.

Disclaimer
This publication is for general information purposes only. It does not purport to provide comprehensive full legal or other advice. Global Legal Group Ltd. and the contributors accept no responsibility for losses that may arise from reliance upon information contained in this publication.
This publication is intended to give an indication of legal issues upon which you may need advice. Full legal advice should be taken from a qualified professional when dealing with specific situations.

© Published and reproduced with kind permission by Global Legal Group Ltd, London

Expert Analysis Chapters

Q&A Chapters

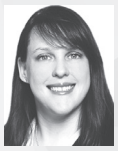
© Published and reproduced with kind permission by Global Legal Group Ltd, London

Q&A Chapters Continued

ICLG.com

© Published and reproduced with kind permission by Global Legal Group Ltd, London

Canada



Lyndsay A. Wasser

Kristen Pennington

McMillan LLP

1 Relevant Legislation and Competent Authorities

1.1 What is the principal data protection legislation?

The *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5 ("**PIPEDA**"), applies to the collection, use and disclosure of employee personal information ("**PI**") by federally regulated employers, as well as PI handled in the course of a Commercial Activity (as defined at question 2.1), except in provinces that have substantially similar legislation.

Three provinces have legislation of general application to the private sector, which are substantially similar to PIPEDA and apply to the collection, use and disclosure of both employee PI and non-employee PI within these provinces:

- Alberta – *Personal Information Protection Act*, SA 2003, c P-6.5 ("**Alberta PIPA**");
- British Columbia ("**B.C.**") – Personal Information Protection Act, SBC 2003, c 63 ("**B.C. PIPA**"); and
- Quebec – *Act respecting the protection of personal information in the private sector*, CQLR c P-39 ("**Quebec Act**").

Collectively, PIPEDA, Alberta PIPA, B.C. PIPA and the Quebec Act are referred to herein as the "**Principal Legislation**".

Some of the health privacy statutes described at question 2.3 below are also substantially similar to PIPEDA, and therefore apply to certain healthcare providers or institutions within those provinces instead of PIPEDA.

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

Yes; the provinces of B.C., Saskatchewan, Manitoba, Newfoundland and Labrador have each enacted statutory torts if a person wilfully violates the privacy of another.

The *Canadian Criminal Code*, RSC 1985, c C-46, includes various offences involving misuse of PI, including hacking, mischief, fraud, identity theft and circumventing technological protection measures.

The *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*, SC 2010, c 23, commonly referred to as "Canada's Anti-Spam Legislation" ("**CASL**"), addresses certain matters involving the collection and use of email addresses as well as interference with computer systems.

Quebec's Act *to establish a legal framework for information technology*, CQLR c C-1.1 ("**Quebec's IT Act**"), requires that certain measures be taken to protect confidential information stored in electronic documents and format, and sets out rules governing the use, retention and transmission of electronic data, including biometric information.

Sections 35 through to 41 of Quebec's *Civil Code*, CQLR c CCQ-1991, govern an individual's right for his reputation and privacy to be respected, as well as unlawful invasions of privacy. Quebec's *Charter of Human Rights and Freedoms*, CQLR c C-12, also contains provisions related to privacy, including Section 5 (the right to respect for one's private life) and Section 46 (the right to fair and reasonable conditions of employment, which can restrict intrusions on employees' privacy).

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

Yes; the *Privacy Act*, RSC, 1985, c P-21 ("**Privacy Act**"), applies to PI processed by federal government institutions. Each Canadian jurisdiction also has legislation that applies to PI handled by public bodies or institutions within the relevant province or territory.

Most provinces and territories have legislation that applies to the processing of personal health information by certain types of custodians, such as doctors and hospitals.

Most provinces also have consumer protection legislation, which includes provisions requiring consumer reporting agencies to ensure the accuracy of, limit the disclosure of, and give consumers access to their PI.

The federal *Bank Act*, RSC 1985, c C-44 ("**Bank Act**") provides for the protection of all registers and records required or authorised under the *Bank Act*, which includes certain customer records. Similarly, Quebec has credit union legislation which requires credit unions to keep customer information confidential and secure.

Some industry regulators or associations have issued guidance and/or established regulatory requirements relating to data protection, including:

- the Canadian Securities Administrators ("**CSA**");
- the Officer of the Superintendent of Financial Institutions ("**OSFI**");
- the Investment Industry Regulatory Organization ("**IIROC**"); and
- the Mutual Fund Dealers Association of Canada ("**MFDA**").

© Published and reproduced with kind permission by Global Legal Group Ltd, London

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

Compliance with PIPEDA and the *Privacy Act* is overseen by the Office of the Privacy Commissioner of Canada ("**OPC**"), and certain offences can be prosecuted by the Attorney General.

Each province and territory also has a regulator responsible for enforcing the privacy statutes in their jurisdiction.

2 Definitions

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

- "**Personal Data**"
  The Principal Legislation uses the term PI, which refers to information about an identifiable individual. This has been interpreted to include any information where there is a serious possibility that an individual could be identified through the use of the information, either alone or in combination with other information.
- "**Processing**"
  This term is not defined in the Principal Legislation, which refers instead to the collection, use and disclosure of PI.
- "**Controller**"
  This term is not used in the Principal Legislation. Some obligations apply to the organisation in control of PI (e.g., breach reporting and recording requirements). An organisation is responsible for PI in its possession or custody, including information that has been transferred to a third party for processing.
- "**Processor**"
  This term is not used in the Principal Legislation. With few exceptions, the Principal Legislation generally does not distinguish between organisations that control PI and those that process PI.
- "**Data Subject**"
  This term is not used in the Principal Legislation. The Principal Legislation governs the processing of the PI of "individuals" (i.e., natural persons).
- "**Sensitive Personal Data**"
  This term is not defined in the Principal Legislation. While some categories of PI will almost always be considered sensitive (e.g., health or financial information), any PI can be considered sensitive depending on the context (taking into account the circumstances and what that information is capable of revealing when combined with other PI regarding the individual).
- "**Data Breach**"
  The equivalent term in PIPEDA is "breach of security safeguards", which refers to the loss of, unauthorised access to, or unauthorised disclosure of PI resulting from a breach of the safeguards required by PIPEDA or failure to establish such safeguards.
- *Other key definitions – please specify (e.g., "Pseudonymous Data", "Direct Personal Data", "Indirect Personal Data")*
  - "Business Contact Information" includes information that is used for the purpose of communicating or facilitating communication with an individual in relation to their employment, business or profession, such as their name, position name or title, or work address, telephone number, fax number or email. Most provisions of the Principal Legislation do not apply to Business Contact Information.
  - Under PIPEDA, "Commercial Activity" refers to a transaction, act or conduct, or any regular course of conduct, that is of a commercial character, including the selling, bartering or leasing of donor, membership or other fundraising lists.

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?

Yes; the Principal Legislation may apply to organisations outside of Canada in some circumstances.

For example, PIPEDA applies to foreign organisations processing PI that have a "real and substantial connection" to Canada. This is a fact-specific analysis that can take into account a variety of factors, including whether the organisation's products or services are specifically marketed to Canadians, whether the PI being processed is about Canadians, and whether any misuse or breach of PI would have an impact on Canadians (for example, by causing them distress, embarrassment or reputational harm).

4 Key Principles

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

- **Transparency**
  Organisations must make readily available to individuals, in a form that is generally understandable, specific information regarding their policies and practices with respect to PI.
- **Lawful basis for processing**
  The Principal Legislation is primarily consent-based. The knowledge and consent of the individual are required for the collection, use or disclosure of their PI, with limited exceptions. Even with consent, organisations must only collect, use and disclose PI for purposes that a reasonable person would consider appropriate in the circumstances.
- **Purpose limitation**
  At or before the time when PI is collected, organisations must generally identify and document the purposes for which such PI will be collected, used and disclosed. Subject to certain limited exceptions, PI cannot be used or disclosed for purposes other than those for which it was collected without the consent of the individual.
- **Data minimisation**
  Both the amount and type of PI must generally be limited to what is necessary for the purposes identified by the organisation when collecting the PI.
- **Proportionality**
  Organisations cannot, as a condition of supplying a product or service, require an individual to consent to the collection, use or disclosure of their PI beyond what is required to fulfil specific and legitimate purposes.
- **Retention**
  PI can generally only be retained for as long as is necessary to fulfil the purposes for which it was collected, at which point it should be destroyed, erased or made anonymous. PI that has been used to make a decision about an individual must be retained long enough to permit the individual to access the PI after the decision has been made (in B.C., at least one year).

© Published and reproduced with kind permission by Global Legal Group Ltd, London

- *Other key principles – please specify*
  - **Accountability**
    As further described at section 7 below, an organisation is responsible for PI under its control and must designate an individual or individuals who are accountable for the organisation's compliance with the Principal Legislation. Organisations must also implement certain policies and practices to give effect to their obligations under the Principal Legislation.
  - **Safeguards**
    Organisations are required to safeguard PI using reasonable physical, organisational and technological measures, which must be appropriate based on the sensitivity of the information as well as the amount, distribution, and format of the information, and the method of storage.

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**
  Individuals generally have the right to be informed of the existence, use and disclosure of their PI and to request access to their PI, subject to certain exceptions. Where access to PI is denied, the reasons for such denial must typically be provided.
- **Right to rectification of errors**
  If an individual successfully demonstrates that their PI is inaccurate or incomplete, the organisation usually must amend the PI and/or add a notation, as appropriate.
- **Right to deletion/right to be forgotten**
  The Principal Legislation does not currently provide for a specific right to deletion of PI or a right to be forgotten. However, giving effect to an individual's request to correct their PI and/or compliance with requirements to retain information only for the period that it is required to fulfil the purposes that it was collected may require deletion of some PI at the request of an individual.
- **Right to object to processing**
  See below regarding withdrawal of consent by an individual.
- **Right to restrict processing**
  See below regarding withdrawal of consent by an individual.
- **Right to data portability**
  The Principal Legislation does not currently provide for a right to data portability.
- **Right to withdraw consent**
  An individual can generally withdraw their consent to the collection, use and disclosure of their PI on reasonable notice, subject to legal or contractual restrictions. The organisation must inform the individual of the implications of such withdrawal.
- **Right to object to marketing**
  Under the Principal Legislation, individuals must generally consent to the collection, use and disclosure of their PI, including for marketing purposes. Use of PI for secondary purposes, including marketing purposes, must be optional (see above under "Proportionality" at question 4.1). CASL also provides that consent is required to send commercial electronic messages ("**CEM**"), and every CEM must contain an unsubscribe mechanism that can be readily performed by the individual.
- **Right to complain to the relevant data protection authority(ies)**
  Individuals have the right to file a complaint with the relevant privacy regulator(s).
- **Other key rights – please specify**
  Individuals also have a right to challenge compliance with the Principal Legislation by submitting a complaint to the organisation itself. Organisations must put in place easily accessible and simple to use procedures to receive and respond to complaints or inquiries regarding their handling of PI.

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, no; however, under Quebec's IT Act, the creation or existence of a database of biometric characteristics and measurements must be disclosed to the *Commission d'accès à l'information* ("**Quebec Commission**"), whether or not the database is in service (the "**Quebec Disclosure Obligation**"). The Quebec Commission may make orders determining how such databases are to be set up, used, consulted, released and retained, and how measurements or characteristics recorded for personal identification purposes are to be archived or destroyed.

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)?

A mandatory form must be filed with the Quebec Commission prior to establishing the Quebec biometric information database.

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

Disclosure must be made for each Quebec biometric information database.

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)?

A representative of the organisation establishing the Quebec biometric information database must sign the mandatory form and attest to the truth of its contents.

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)?

The mandatory form that must be filed with respect to a Quebec biometric information database includes information such as the

© Published and reproduced with kind permission by Global Legal Group Ltd, London

number of people affected, the types of biometric information gathered, the objective of gathering the information, and a copy of the method of obtaining consent.

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

The Quebec Commission may suspend, prohibit the bringing into service or order the destruction of a database of biometric characteristics and measurements if the database is not in compliance with the orders of the Quebec Commission or otherwise constitutes an invasion of privacy.

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

There is no fee per registration/notification.

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

Provided there are no material changes to the biometric database, disclosure must only be made once per database.

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

As set out at question 6.1, disclosure to the Quebec Commission must be made prior to bringing the biometric database into service.

6.10 Can the registration/notification be completed online?

Yes; the registration/notification can be completed online.

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

No; there is not a publicly available list of completed registrations/notifications.

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

This information is not publicly available. However, the Quebec Commission recommends that the required form be submitted as early as possible to allow for sufficient processing time.

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, Alberta PIPA and B.C. PIPA require organisations to designate an individual or individuals to be accountable for the organisation's compliance with the legislation ("**DPO**").

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

There are currently no particular sanctions for failing to appoint a DPO. However, as set out at question 15.4, Alberta PIPA generally allows for fines where an organisation collects, uses or discloses PI in contravention of Alberta PIPA, and these fines could be applied to an organisation that fails to appoint a DPO.

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

The Principal Legislation contains anti-reprisal provisions that prohibit organisations from denying a benefit or taking adverse employment action against any employee (whether or not they are the DPO) because that employee has done or has said they will do something to avoid a contravention of the legislation.

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

Yes; a business can appoint a single DPO to cover multiple entities.

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

There are no statutory qualification requirements for the DPO; however, regulatory guidance indicates that they should have the support of the organisation's senior management and the authority to intervene on privacy-related issues.

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

The Principal Legislation broadly requires that the DPO is accountable for the organisation's compliance with the legislation.

Getting Accountability Right with a Privacy Management Program – guidance jointly published by the OPC, the Office of the Information and Privacy Commissioner of Alberta (the "**Alberta Regulator**") and the Office of the Information & Privacy Commissioner for B.C. (the "**B.C. Regulator**") – describes the DPO's responsibilities as structuring, designing and managing the organisation's privacy management programme, including all procedures, training, monitoring/auditing, documenting, evaluating, and follow-up. Other responsibilities include: establishing and implementing privacy management programme controls; coordinating with persons responsible for related discipline and functions within the organisation; ongoing assessment and revision of programme controls; representing the organisation in the event of an investigation by a regulator; and advocating about privacy within the organisation.

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

No; the appointment of a DPO does not need to be registered with or notified to the relevant data protection authority(ies).

© Published and reproduced with kind permission by Global Legal Group Ltd, London

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

PIPEDA requires that the identity of the DPO be made known upon request.

B.C. PIPA and Alberta PIPA also require that, on request, an organisation provide the name or title of the person who can answer questions regarding the organisation's collection, use, disclosure or storage of PI. Alberta PIPA also requires that this information be provided before or at the time PI is collected.

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?

An organisation that transfers PI to a third party for processing remains responsible for the PI and must use contractual or other means to protect such PI.

See section 11 below for additional considerations regarding the engagement of service providers that process PI outside of Canada.

Where applicable, public and health sector privacy legislation may also require organisations to enter into data sharing agreements with service providers.

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.)?

The Principal Legislation does not prescribe the specific contents of a data protection agreement.

Joint guidance from the OPC, Alberta Regulator and B.C. Regulator provides that, at a minimum, agreements with service providers should include provisions that: (i) set out requirements for compliance, including binding the service provider to the policies and protocols of the organisation; (ii) require the organisation to be notified in the event of a data breach; (iii) require training and education for all service provider employees with access to PI; (iv) address subcontracting; (v) address audit rights; and (vi) require agreements with service provider employees stating that they will comply with the organisation's privacy policies and protocols.

Some industry-specific privacy laws, such as health privacy legislation, prescribe specific requirements for data protection agreements with certain service providers.

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?).

In addition to being governed by the Principal Legislation, the sending of CEMs must comply with CASL in all respects. CASL requires consent to send, or cause or permit to be sent, a CEM to an electronic address. Consent must generally opt-in (upon providing certain disclosures); however there are some narrow exceptions where it may be implied for limited time periods. CASL also sets out the minimum content of CEMs, including (without limitation) the unsubscribe mechanism described at question 5.1.

9.2 Are these restrictions only applicable to business-to-consumer marketing, or do they also apply in a business-to-business context?

CASL will generally apply in a business-to-business context where CEMs are sent to electronic addresses. However, certain exceptions may apply to some business activities, for example where CEMs are sent to a person who is engaged in a commercial activity and the CEMs consist solely of an inquiry or application related to that activity.

9.3 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.).

Both telephone and postal marketing must comply with the Principal Legislation in all respects.

Canada's *Unsolicited Telecommunications Rules* ("**UTR**") include additional requirements that apply to marketing by telephone. The *Telecommunications Act*, SC 1993, c 38, also establishes a National Do Not Call List ("**NDNCL**") of individuals who have registered not to receive unsolicited marketing communications by telephone or fax. Telemarketers cannot initiate, and their clients must make all reasonable efforts to ensure that they do not initiate, telemarketing telecommunications to those on the NDNCL, absent express consent.

Organisations that initiate telemarketing telecommunications on their own behalf or as a client of a telemarketer must also maintain and respect their own internal "do not call" lists.

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

Yes; the restrictions noted above apply to marketing sent from other jurisdictions.

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

Yes; breaches of these marketing restrictions are enforced by several regulators, including the OPC, provincial privacy regulators, the Competition Bureau and the Canadian Radio-Television and Telecommunications Commission.

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

Organisations wishing to purchase marketing lists must ensure that individuals' meaningful consent has been obtained for the collection, use and disclosure of their PI by all relevant parties for marketing purposes.

The OPC's *Guidance for businesses doing e-marketing* recommends that, prior to purchasing or using a marketing list, organisations should ask for a detailed explanation of how: the email addresses were gathered; consent was originally obtained; the list is kept up to date; the vendor ensures that PI is promptly deleted from

© Published and reproduced with kind permission by Global Legal Group Ltd, London

the list when consent is withdrawn; and the vendor will inform the organisation of any changes to the list.

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

Persons who contravene the requirements of CASL may be subject to administrative penalties of up to $1 million for individuals and $10 million for any other person.

Persons who contravene the UTR may also be subject to penalties of up to $1,500 per violation for an individual and up to $15,000 per violation for a corporation.

See question 15.4 for a description of potential fines for organisations that collect, use or disclose PI in contravention of Alberta PIPA or the Quebec Act.

10 Cookies

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

The OPC has taken the position that information collected about individuals' web activities by means of technologies such as cookies may constitute PI and therefore be subject to PIPEDA. Other regulators may take a similar position; therefore, the use of cookies should comply with any applicable privacy laws.

In its *Policy position on online behavioural advertising*, the OPC sets out specific considerations related to the use of online behavioural advertising ("**OBA**"), including conditions that must be satisfied in order for an organisation to rely on individuals' implied consent to the collection, use and disclosure of their non-sensitive PI for OBA. For example, individuals must be made aware of the purposes of the OBA in a clear and understandable manner at or before the time of collection and must be able to easily opt-out of the OBA with immediate and persistent effect.

Under CASL, a person is generally prohibited from installing a computer program on another person's computer system, unless they have the express consent of the other person to do so. A person is considered to consent to the installation of a computer program if the person's conduct is such that it is reasonable to believe that they consent.

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

The OPC takes the position that zombie cookies, supercookies, third-party cookies that appear to be first-party cookies, device fingerprinting and other techniques that cannot be controlled by individuals are not permitted pursuant to PIPEDA as they do not permit individuals to effectively opt-out of the collection and use of their PI.

The OPC also takes the position that organisations should avoid knowingly tracking children, including by using cookies or other tracking technologies on websites aimed at children.

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

Yes; there have been several regulatory investigations in relation to cookies.

For example, in PIPEDA Case Summary #2003-162, the OPC found that requiring users to consent to permanent cookies as a condition of accessing a website was a contravention of PIPEDA.

In PIPEDA Report of Findings #2013-003, the OPC reiterated that organisations must disclose to website visitors the use of cookies and the purposes for which the organisation collects PI.

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

As noted at questions 9.7 and 15.4, CASL, Alberta PIPA and the Quebec Act allow for the imposition of administrative penalties or fines, which could be levied in the event of non-compliance related to cookies.

11 Restrictions on International Data Transfers

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

The Principal Legislation generally allows for the transfer of PI to other jurisdictions if the organisation uses contractual or other means to provide a comparable level of protection while the PI is being processed abroad. However, certain restrictions and requirements may apply.

Organisations must assess risks that could jeopardise the integrity, security and confidentiality of PI when it is transferred outside of Canada. For example, the OPC has taken the position that the PI of individuals who purchase cannabis should generally be stored on a server located in Canada because cannabis use is illegal in most other countries. Organisations subject to PIPEDA must also advise individuals that their PI may be sent to another jurisdiction for processing and may be accessed by foreign courts, law enforcement and national security authorities.

Under Alberta PIPA, an organisation who uses a service provider (including a parent corporation, subsidiary or affiliate) outside of Canada to collect, use, disclose or store PI must have policies and practices regarding: (i) the countries outside Canada in which the collection, use, disclosure or storage of PI is occurring or may occur; and (ii) the purposes for which the service provider outside Canada has been authorised to collect, use or disclose PI for or on behalf of the organisation. The organisation must, prior to or at the time of collecting or transferring the PI, notify the individual of the way in which they may obtain written information regarding the organisation's policies and practices with respect to service providers outside of Canada and the name or position/title of a person who is able to answer questions about the collection, use, disclosure or storage of PI by such service providers.

Pursuant to the Quebec Act, prior to communicating or entrusting PI to a person outside of Quebec with the task of holding, using or communicating such PI on the organisation's behalf, an organisation must first take all reasonable steps to ensure: (i) that the PI will not be used for irrelevant purposes or communicated to third parties without the individual's consent; and (ii) in the case of nominative lists, that individuals have a valid opportunity to refuse that their PI be used for purposes of commercial or philanthropic prospection and, if need be, to have such PI deleted from the list. If the organisation determines that this level of protection will not be afforded to the PI,

© Published and reproduced with kind permission by Global Legal Group Ltd, London

the organisation must refuse to communicate or entrust the PI to a party outside of Quebec.

Some public and health sector privacy statutes also include requirements and/or restrictions applicable to transferring PI outside of Canada or the relevant province.

11.2 Please describe the mechanisms businesses 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.).

Organisations typically enter into data processing agreements to ensure that PI transferred outside of Canada is provided a comparable level of protection. While the consent of the individual to such a transfer is not generally required under the Principal Legislation, organisations must satisfy all statutory requirements, including those described at question 11.1.

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.

No, transfers of personal data to other jurisdictions do not require registration with, notification to or prior approval from the relevant data protection authority(ies).

11.4 What guidance (if any) has/have the data protection authority(ies) issued following the decision of the Court of Justice of the EU in *Schrems II* (Case C-311/18)?

To date, Canadian privacy regulators have not released guidance with respect to the *Schrems II* decision. PIPEDA is currently considered "adequate" for the purposes of permitting transfers of personal data from the EU to Canada. In addition, the federal government and Quebec's provincial government have proposed significant reforms to PIPEDA and the Quebec Act, respectively, which, if passed, would align with several of the General Data Protection Regulation's ("GDPR") standards.

11.5 What guidance (if any) has/have the data protection authority(ies) issued in relation to the European Commission's revised Standard Contractual Clauses?

To date, Canadian privacy regulators have not released guidance with respect to the EU Commission's revised standard contractual clauses. See above regarding PIPEDA's adequacy designation.

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.)?

The Principal Legislation does not expressly prohibit or restrict the establishment of whistle-blower hotlines.

An OPC investigation into the use of a whistle-blower system by a government entity suggested that organisations considering using a whistle-blower hotline must balance the expectations of confidentiality and anonymity for reporters with procedural fairness concerns for individuals who are subject to an investigation.

Whistle-blowers within federal institutions are afforded protections by the Public Servants *Disclosure Protection Act*, SC 2005 c 46.

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

To date, Canadian privacy regulators have not issued guidance or investigation reports discouraging or prohibiting anonymous reporting. Accordingly, anonymous reporting is generally permitted.

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)?

There are no requirements for registration, notification or prior approval of the use of CCTV cameras under the Principal Legislation.

However, joint guidance from the OPC, Alberta Regulator and B.C. Regulator provides that organisations must post signs alerting an individual to the presence of a camera before they enter the premises. Such signs should include a contact person in case individuals have questions or want access to their PI that is collected by the camera. Some Canadian privacy regulators have also recommended that the purpose(s) of the cameras should be disclosed.

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

PI collected through CCTV cameras may only be used for purposes that a reasonable person would consider appropriate in the circumstances. According to joint guidance from the OPC, Alberta Regulator and B.C. Regulator, examples of appropriate purposes may include security around banking machines or inside convenience stores in high-crime areas. Organisations should consider less privacy-invasive alternatives before installing CCTV cameras. The B.C. Regulator has also stated that video surveillance should be used only in response to a real and significant security or safety problem.

14 Employee Monitoring

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

Various types of employee monitoring have been upheld by Canadian privacy regulators and adjudicators in certain circumstances, including video surveillance, monitoring employees' use of information technology, recording telephone calls, and GPS tracking. However, such monitoring must be carried out in accordance with applicable privacy laws and may also have employment and labour law implications.

© Published and reproduced with kind permission by Global Legal Group Ltd, London

Canadian privacy regulators and adjudicators have developed different tests to evaluate when employee monitoring is acceptable. Common considerations in assessing whether employee monitoring is reasonable include: (i) whether there is a legitimate issue or demonstrable need to be addressed through the monitoring; (ii) whether the monitoring is likely to be effective in addressing that issue or meeting that need; (iii) whether the loss of privacy is proportional to the benefit gained through the monitoring; and (iv) whether there is a less privacy-invasive way of achieving the same end. In assessing whether the monitoring is reasonable, some privacy regulators and adjudicators have also considered the sensitivity of the PI collected, whether the monitoring is covert, and whether the employee had a subjective expectation of privacy.

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

PIPEDA, Alberta PIPA and B.C. PIPA permit employers to collect, use and disclose employees' PI without their consent, provided such collection, use and disclosure is only for purposes reasonably required to establish, manage or terminate an employment relationship. However, the employer must still provide the individual with advance notice that their PI will be collected, used or disclosed and the purposes for doing so, in addition to complying with all other statutory requirements.

In Quebec, employees' consent to the collection, use and disclosure of their PI through monitoring will generally be required, subject to limited exceptions.

Employers may also be subject to statutory and/or common law tort claims related to employee monitoring, including claims that unreasonable monitoring constitutes an intrusion upon seclusion.

In practice, most employers provide notice and/or obtain consent to collect PI through employee monitoring via employment agreements, policies that are brought to employees' attention (e.g., workplace privacy policies, acceptable use policies, etc.) and/or by using signage in the workplace.

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

Employers should consult the terms of any applicable collective agreements in order to determine whether a union or employee association must be notified of, or consulted with respect to, the implementation of employee monitoring.

Even where such an obligation does not exist by operation of a collective agreement, employers may strategically decide to advise a union or employee association of the implementation of employee monitoring in order to obtain feedback and potentially lower the risk of a policy grievance or other objection once the monitoring is implemented.

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.)?

The Principal Legislation generally requires that an organisation must protect PI against loss or theft, as well as unauthorised access, disclosure, copying, use or modification using physical, organisational and technological measures that are appropriate to the sensitivity of the PI as well as the amount, distribution, and format of the information, and the method of storage.

An organisation that transfers PI to a third party for processing must use contractual or other means to protect such PI, including by ensuring that a processor also implements appropriate safeguards.

Some industry regulators, including the CSA, OSFI, IIROC and MFDA (as defined at question 1.3), require organisations to monitor, detect, prevent and/or mitigate incidents involving PI and other cyber-incidents.

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) expect(s) voluntary breach reporting.

PIPEDA requires an organisation to report to the OPC a loss of, unauthorised access to or unauthorised disclosure of PI resulting from a breach of the organisation's security safeguards or from a failure to establish those safeguards (a "**Breach of Security Safeguards**") where it is reasonable in the circumstances to believe that the Breach of Security Safeguards creates a real risk of significant harm ("**RROSH**") to any individual(s) (a "**Reportable Breach**").

The report must be made as soon as feasible after the organisation determines that a Reportable Breach has occurred, and must be in writing and contain (to the extent known):

- a description of the circumstances of the Reportable Breach and the cause;
- the day on which, or the period during which, the Reportable Breach occurred;
- a description of the PI that is the subject of the Reportable Breach;
- the number of individuals affected by the Reportable Breach;
- a description of the steps that the organisation has taken to reduce the risk of harm to individuals that could result from the Reportable Breach, or to mitigate that harm;
- a description of the steps that the organisation has taken or intends to take to notify affected individuals of the Reportable Breach; and
- the name and contact information of a person who can answer the OPC's questions about the Reportable Breach.

PIPEDA also requires organisations to advise any organisation or governmental institution that may be able to reduce or mitigate the risk of harm arising from the Reportable Breach.

Alberta PIPA also requires that an organisation having PI under its control provide notice, without unreasonable delay, to the Alberta Regulator of any incident involving the loss of or unauthorised access to or disclosure of PI where a reasonable person would consider that there exists a RROSH to an individual as a result of the loss or unauthorised access or disclosure. The contents of the notice are prescribed by Section 19 of the *Personal Information Protection Act Regulation*, Alta Reg 366/2003.

The B.C. Regulator and the Quebec Commission also generally expect voluntary reporting of breaches that give rise to a RROSH.

Public sector legislation and health sector legislation in some provinces and territories also include breach reporting requirements.

Some industry regulators, including the CSA, OSFI, IIROC and MFDA (as defined at question 1.3), require organisations to report or disclose certain breaches/incidents to the regulators.

© Published and reproduced with kind permission by Global Legal Group Ltd, London

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) expect(s) voluntary breach reporting.

PIPEDA requires that organisations notify individuals of any Reportable Breach as soon as feasible. Such notice must contain sufficient information to enable individuals to understand the significance of the Reportable Breach to them and to take steps to reduce or mitigate the risk of harm, and must also contain certain prescribed content, including (without limitation) a description of the Reportable Breach, timing of the Reportable Breach, the PI impacted and the steps taken by the organisation to mitigate or reduce the risk of harm.

Under Alberta PIPA, the Alberta Regulator can require an organisation to notify individuals to whom there is a RROSH as a result of a breach. The contents of the notice (if required) are prescribed by Section 19.1(1) of the *Personal Information Protection Act Regulation*, Alta Reg 366/2003.

The B.C. Regulator and the Quebec Commission also generally expect voluntary notification of breaches that give rise to a RROSH, and failure to do so can increase litigation risk.

15.4 What are the maximum penalties for data security breaches?

The OPC can make non-binding recommendations in the event of non-compliance with PIPEDA, including a failure to implement adequate safeguards to protect PI from Breaches of Security Safeguards. Following the OPC's issuance of recommendations, an application can be made to the Federal Court for relief, including damages to complainants. The Attorney General can prosecute an organisation for failing to comply with the breach reporting, notification and recording obligations under PIPEDA, which can result in fines of up to $10,000 on summary conviction or $100,000 for an indictable offence.

Under Alberta PIPA, an organisation that collects, uses or discloses PI in contravention of Alberta PIPA, or that fails to comply with its breach reporting obligations, can be subject to fines up of to $10,000 for an individual or $100,000 for a person other than an individual.

Under the Quebec Act, an organisation that collects, holds, communicates to third parties or uses PI in contravention of the Quebec Act is liable to a fine of $1,000 to $10,000 for a first offence and $10,000 to $20,000 for a subsequent offence.

Individuals whose PI is compromised by a privacy or security breach can also bring civil tort claims for damages, either on an individual basis or as part of a class action proceeding.

16 Enforcement and Sanctions

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

(a) **Investigative Powers**: Canadian privacy regulators are generally empowered to conduct investigations into organisations' compliance with the Principal Legislation. The scope of the regulators' investigative powers is set out in the applicable legislation, and may include, for example, the ability to compel oral or written evidence under oath, enter certain premises, and obtain or compel the production of certain records. Some regulators are also empowered to order or initiate mediation, hearings and/or inquiries into complaints of non-compliance with privacy legislation and/or to enter into voluntary compliance agreements with organisations that have been found to have contravened privacy legislation.

(b) **Corrective Powers**: At the conclusion of an investigation under PIPEDA, the OPC will typically issue a report of findings, including the conclusions of its investigation and non-binding recommendations to rectify and prevent the reoccurrence of non-compliance. Following the OPC's report, an application can be made to the Federal Court, where a variety of remedial orders (including damages to complainants) can be issued. Both the Alberta Regulator and B.C. Regulator can issue binding orders against an organisation following an inquiry. If such an order is issued, both Alberta PIPA and B.C. PIPA provide that (an) affected individual(s) can bring an action against the organisation for damages for loss or injury caused by the organisation's actions. The Quebec Act provides that, following an inquiry, the Quebec Commission may recommend or order the application of such remedial measures as are appropriate to ensure the protection of PI.

(c) **Authorisation and Advisory Powers: Canadian privacy regulators may play a variety of advisory roles, for example by**: (i) providing independent reviews and resolutions of requests and complaints related to access to information requests and the handling of PI; (ii) advising and making recommendations about the application of privacy legislation to stakeholders; and (iii) commenting on the privacy implications of proposed legislation, programmes or policies or new technologies. The regulators also publish guidance documents (often jointly) regarding the interpretation and application of privacy and data protection laws.

(d) **Imposition of administrative fines for infringements of specified GDPR provisions**: Canadian privacy regulators are not empowered to impose administrative fines for non-compliance with the GDPR. However, as set out at questions 15.4 and 16.1(e), some regulators may be able to issue fines for infringements of the Principal Legislation.

(e) **Non-compliance with a data protection authority**: Under PIPEDA, if an organisation fails to abide by the terms of a voluntary compliance agreement with the OPC, the OPC may apply to the Federal Court for relief, including an order requiring the organisation to comply with the terms of the compliance agreement. In Alberta, an order of the Alberta Regulator can be filed with the Court of Queen's Bench and thereafter becomes enforceable as a judgment or order of that court. Failing to comply with an order of the Alberta Regulator is an offence and is subject to the maximum penalties set out at question 15.4. A person who fails to comply with an order of the B.C. Regulator is guilty of an offence and is liable, if an individual, to a fine of not more than $10,000, and, if a person other than an individual, to a fine of not more than $100,000. An order of the Quebec Commission can also be filed and executed as a judgment of Quebec's Superior Court.

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?

As set out at question 16.1, Canadian privacy regulators generally have the ability to make recommendations or issue orders, including, in some cases, requiring an organisation to stop collecting, using or disclosing PI in contravention of the

© Published and reproduced with kind permission by Global Legal Group Ltd, London

Principal Legislation. Enforcing such a recommendation or order may require the regulator to either file the order with the court or, in the case of PIPEDA, apply to the Federal Court for relief.

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

The OPC and provincial privacy regulators chiefly take a collaborative approach to resolving privacy complaints, which includes making recommendations and issuing joint reports. The OPC has also worked in coordination with privacy authorities from other countries to arrive at joint findings (see, for example, PIPEDA Report of Findings #2018-003).

On rare occasions, the OPC has entered into voluntary compliance agreements (see PIPEDA Report of Findings #2018-006 and #2016-005). The OPC last applied to the Federal Court for a *de novo* hearing in 2017 (see PIPEDA Report of Findings #2017-007).

Investigations of possible contraventions of Canadian privacy laws can be initiated by complaints from individuals (see PIPEDA Report of Findings #2020-001), following data breach disclosures by organisations (see PIPEDA Report of Findings #2020-005), or, increasingly, by the privacy regulators themselves working proactively (see PIPEDA Report of Findings #2020-004).

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

Yes; see question 3.1.

In *A.T. v. Globe 24h.com*, 2017 FC 114, the Federal Court found that PIPEDA had extraterritorial application to a website operated out of and hosted on a server in Romania because there was a "real and substantial link" between the website's activities and Canada. The fact that Romanian authorities had already acted to curtail the website's activities did not preclude PIPEDA from applying where the activities had unlawful consequences in Canada.

17 E-discovery / Disclosure to Foreign Law Enforcement Agencies

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

Organisations should consult applicable privacy legislation to confirm whether such disclosure of PI is lawful and, if so, whether the individual's consent to such disclosure is required.

For example, PIPEDA provides that an organisation may disclose PI without the knowledge or consent of an individual if: (i) the disclosure is made to a government institution (or part of a government institution) that has made a request for the PI, identified its lawful authority to obtain the PI, and indicated that the disclosure is requested for the purpose of enforcing any law of a foreign jurisdiction, carrying out an investigation relating to the enforcement of any such law or gathering intelligence for the purpose of enforcing any such law; or (ii) the disclosure is required to comply with a subpoena or warrant issued or an order made by a court, person or body with jurisdiction to compel the production of information, or to comply with rules of court relating to the production of records.

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

In its *Guidelines for Processing Personal Data Across Borders*, the OPC advises that organisations that transfer PI outside of Canada for processing must make it plain to individuals that their PI may be processed in a foreign country and, therefore, may be accessible to law enforcement and national security authorities of that jurisdiction. Organisations must do this in clear and understandable language, typically at the time the PI is collected.

In *PIPEDA and Your Practice: A Privacy Handbook for Lawyers*, the OPC advises both lawyers and their clients to be particularly sensitive to the requirements of PIPEDA during e-discovery. The OPC notes that Canadian courts have repeatedly rejected requests for production of entire hard drives and other electronic information on the grounds that such production constitutes an unjustified invasion of privacy. Courts can also impose privacy-protective measures to ensure that the invasion of privacy is kept to a minimum. Lawyers and clients who hire service providers to assist in managing e-discovery issues must also satisfy themselves that those service providers will comply with PIPEDA, including by using contractual or other means to ensure that PI receives a comparable level of protection while being processed by the service provider and giving notice to individuals if their PI will be processed outside of Canada (however, the OPC recognises that the latter may not be feasible with respect to PI received from an opposing party during e-discovery).

18 Trends and Developments

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

In the past year, Canadian privacy regulators have combined their resources to conduct several joint investigations, including:

- an investigation by the OPC, the Alberta Regulator and the B.C. Regulator into the collection and use of PI (including biometric information) of visitors to malls via anonymous video analytics technology installed in wayfinding directories and mobile device geolocation tracking technologies (PIPEDA Report of Findings #2020-004);
- an investigation by the OPC and Quebec Commission into a data breach by an employee that ex-filtrated the PI of close to 9.7 million individuals in Canada and abroad over a period of 26 months (PIPEDA Report of Findings #2020-005); and
- an investigation into the facial recognition tool of Clearview AI, Inc. by the OPC, the Quebec Commission, the Alberta Regulator and the B.C. Regulator (PIPEDA Report of Findings #2021-001).

The OPC has also recently focused on several complaints related to foreign processing of consumers' PI (see, for example, PIPEDA Report of Findings #2020-001 and #2020-003).

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

- **Statutory reform, including stronger enforcement mechanisms** – For several years, the OPC has been advocating for significant reforms to Canadian privacy laws, including enhanced enforcement powers and significant penalties for non-compliant organisations. In November 2020, the federal government tabled Bill C-11 which, if

© Published and reproduced with kind permission by Global Legal Group Ltd, London

passed, would allow for significant administrative penalties for organisations that contravene federal privacy legislation, as well as establish a tribunal to adjudicate appeals from OPC orders. The provincial governments of Quebec and B.C. are also considering changes to strengthen their privacy legislation.

- **Privacy implications of new technologies** – Recent cases indicate that regulators are focused on the privacy impact of new technologies, including (without limitation) automatic scanning tools and the use of artificial intelligence.
- **Transborder dataflows** – International data processing has been a "hot topic" for several years, and Canada's approach to this issue is far from finalised.
- **Health privacy** – With new advances in online healthcare, health privacy issues are likely to be an area of interest to Canadian privacy regulators.

Acknowledgment

Lyndsay and Kristen are grateful to Robbie Grant for his research and assistance with this chapter.

© Published and reproduced with kind permission by Global Legal Group Ltd, London

Lyndsay A. Wasser is the Co-Chair of McMillan's Privacy & Data Protection Group and its Cybersecurity Group. She is a Certified Information Privacy Professional/Canada and regularly advises and assists clients on a broad range of privacy and cybersecurity issues, including advising on legal requirements related to data security, workplace privacy issues, handling personal health information and transferring PI across borders. She assists clients to develop privacy compliance programmes and data sharing agreements. She has assisted many clients with responding to privacy and data breaches involving various types of information (e.g., payment card information, patient data, employee personal information and sensitive identity information), including assisting with risk assessment, breach response strategy, notification obligations and communications with regulators. Lyndsay regularly writes and speaks on cybersecurity topics and is the co-author of *Privacy in the Workplace*, 4th ed. and the privacy chapter in the *Ultimate Corporate Counsel Guide*.

McMillan LLP
Brookfield Place, Suite 4400
181 Bay Street
Toronto, Ontario
Canada
M5J 2T3

Tel: +1 416 865 7083
Email: lyndsay.wasser@mcmillan.ca
URL: www.mcmillan.ca

Kristen Pennington is a Partner in McMillan's Privacy & Data Protection and Cybersecurity Groups. Kristen advises organisations about legal requirements related to privacy and data protection, including employee background checks, cross-border transfers of personal information and the privacy implications of corporate transactions. She assists clients with developing practical, up-to-date privacy compliance programmes and with drafting appropriate waivers, consent forms and data sharing terms with service providers, affiliates and other third parties. An experienced advocate, Kristen has appeared before the Ontario Superior Court and the Ontario Court of Appeal and at various mediations. Kristen regularly writes and speaks about emerging Canadian privacy topics, including the rise of privacy torts in Canada and the processing of employee and third-party personal information in connection with COVID-19.

McMillan LLP
Brookfield Place, Suite 4400
181 Bay Street
Toronto, Ontario
Canada
M5J 2T3

Tel: +1 416 865 7943
Email: kristen.pennington@mcmillan.ca
URL: www.mcmillan.ca

McMillan is a leading Canadian business law firm with recognised expertise and acknowledged leadership in major business sectors, which provides solutions-oriented legal advice through its offices in Calgary, Montréal, Ottawa, Toronto, Vancouver and Hong Kong. McMillan's privacy law experts have a thorough understanding of legal and regulatory obligations related to privacy, data protection and cybersecurity, and regularly assist organisations by: advising on compliance with applicable privacy and data protection, anti-spam, misleading advertising and other legislation; drafting data protection policies, protocols and training materials; negotiating agreements with third-party suppliers and service providers while analysing privacy and data protection implications; strategic handling of data breaches; assisting vendors and purchasers with assessing the privacy law implications of corporate transactions; and advising on and defending claims related to data protection, including defending class action litigation.

www.mcmillan.ca

© Published and reproduced with kind permission by Global Legal Group Ltd, London

ICLG.com

Other titles in the ICLG series

Alternative Investment Funds
Anti-Money Laundering
Aviation Finance & Leasing
Aviation Law
Business Crime
Cartels & Leniency
Class & Group Actions
Competition Litigation
Construction & Engineering Law
Consumer Protection
Copyright
Corporate Governance
Corporate Immigration
Corporate Investigations
Corporate Tax
Cybersecurity
Derivatives
Designs
Digital Business
Digital Health
Drug & Medical Device Litigation
Employment & Labour Law
Enforcement of Foreign Judgments
Environment & Climate Change Law
Environmental, Social & Governance Law
Family Law
Fintech
Foreign Direct Investment Regimes
Franchise
Gambling
Insurance & Reinsurance
International Arbitration
Investor-State Arbitration
Lending & Secured Finance
Litigation & Dispute Resolution
Merger Control
Mergers & Acquisitions
Mining Law
Oil & Gas Regulation
Patents
Pharmaceutical Advertising
Private Client
Private Equity
Product Liability
Project Finance
Public Investment Funds
Public Procurement
Real Estate
Renewable Energy
Restructuring & Insolvency
Sanctions
Securitisation
Shipping Law
Technology Sourcing
Telecoms, Media & Internet
Trade Marks
Vertical Agreements and Dominant Firms

@ICLG_GLG

The International Comparative Legal Guides are published by:

global legal group