



ICLG

The International Comparative Legal Guide to: **Data Protection 2017**

4th Edition

A practical cross-border insight into data protection law

Published by Global Legal Group, with contributions from:

Affärsadvokaterna i Sverige AB

Bae, Kim & Lee LLC

Bagus Enrico & Partners

Creel, García-Cuellar, Aiza y Enríquez, S.C.

Cuatrecasas

Dittmar & Indrenius

Drew & Napier LLC

Ecija Abogados

ErsoyBilgehan

Eversheds Sutherland

GANADO Advocates

Gilbert + Tobin

GRATA International

Hacohen & Co.

Herbst Kinsky Rechtsanwälte GmbH

Hunton & Williams

Koushos Korfiotis Papacharalambous LLC

Lee and Li, Attorneys-at-Law

LPS L@w

Matheson

Mori Hamada & Matsumoto

Osler, Hoskin & Harcourt LLP

Pachiu & Associates

Pestalozzi Attorneys at Law Ltd.

Portolano Cavallo

Rato, Ling, Lei & Cortés Lawyers

Rossi Asociados

Subramaniam & Associates (SNA)

Wikborg Rein Advokatfirma AS



Contributing Editors
Anita Bapat and Aaron
P. Simpson, Hunton & Williams

Sales Director
Florjan Osmani

Account Director
Oliver Smith

Sales Support Manager
Paul Mochalski

Sub Editor
Hollie Parker

Senior Editors
Suzie Levy, Rachel Williams

Chief Operating 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
May 2017

Copyright © 2017
Global Legal Group Ltd.
All rights reserved
No photocopying

ISBN 978-1-911367-50-5
ISSN 2054-3786

Strategic Partners



General Chapter:

1	All Change for Data Protection: The European Data Protection Regulation – Bridget Treacy & Anita Bapat, Hunton & Williams	1
---	--	---

Country Question and Answer Chapters:

2	Australia	Gilbert + Tobin: Melissa Fai & Alex Borowsky	7
3	Austria	Herbst Kinsky Rechtsanwälte GmbH: Dr. Sonja Hebenstreit & Dr. Isabel Funk-Leisch	23
4	Belgium	Hunton & Williams: Wim Nauwelaerts & David Dumont	34
5	Canada	Osler, Hoskin & Harcourt LLP: Adam Kardash & Brandon Kerstens	43
6	Chile	Rossi Asociados: Claudia Rossi	53
7	China	Hunton & Williams: Manuel E. Maisog & Judy Li	60
8	Cyprus	Koushos Korfiotis Papacharalambous LLC: Anastasios Kareklas & Georgia Charalambous	67
9	Finland	Dittmar & Indrenius: Jukka Lång & Iris Keino	76
10	France	Hunton & Williams: Claire François	84
11	Germany	Hunton & Williams: Anna Pateraki	93
12	India	Subramaniam & Associates (SNA): Hari Subramaniam & Aditi Subramaniam	105
13	Indonesia	Bagus Enrico & Partners: Enrico Iskandar & Bimo Harimahesa	117
14	Ireland	Matheson: Anne-Marie Bohan & Andreas Carney	125
15	Israel	Hacohen & Co.: Yoram Hacohen	138
16	Italy	Portolano Cavallo: Laura Liguori & Adriano D'Ottavio	147
17	Japan	Mori Hamada & Matsumoto: Hiromi Hayashi & Rina Shimada	156
18	Kazakhstan	GRATA International: Leila Makhmetova & Saule Akhmetova	167
19	Korea	Bae, Kim & Lee LLC: Tae Uk Kang & Susan Park	176
20	Macau	Rato, Ling, Lei & Cortés Lawyers: Pedro Cortés & José Filipe Salreta	185
21	Malta	GANADO Advocates: Dr. Paul Micallef Grimaud & Dr. Philip Mifsud	194
22	Mexico	Creel, García-Cuéllar, Aiza y Enríquez, S.C.: Begoña Cancino Garín	202
23	Norway	Wikborg Rein Advokatfirma AS: Dr. Rolf Riisnæs & Dr. Emily M. Weitzenboeck	209
24	Portugal	Cuatrecasas: Leonor Chastre	220
25	Romania	Pachiu & Associates: Mihaela Cracea & Alexandru Lefter	231
26	Russia	GRATA International: Yana Dianova	242
27	Senegal	LPS L@w: Léon Patrice Sarr & Ndéye Khady Youm	255
28	Singapore	Drew & Napier LLC: Lim Chong Kin & Charmian Aw	263
29	South Africa	Eversheds Sutherland: Tanya Waksman	273
30	Spain	Ecija Abogados: Carlos Pérez Sanz & Pia Lestrade Dahms	281
31	Sweden	Affärsadvokaterna i Sverige AB: Mattias Lindberg	291
32	Switzerland	Pestalozzi Attorneys at Law Ltd.: Michèle Burnier & Lorenza Ferrari Hofer	300
33	Taiwan	Lee and Li, Attorneys-at-Law: Ken-Ying Tseng & Rebecca Hsiao	310
34	Turkey	ErsoyBilgehan: Zihni Bilgehan & Yusuf Mansur Özer	319
35	United Kingdom	Hunton & Williams: Anita Bapat & Adam Smith	327
36	USA	Hunton & Williams: Aaron P. Simpson & Jenna N. Rode	336

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

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.

Canada



Adam Kardash



Brandon Kerstens

Osler, Hoskin & Harcourt LLP

1 Relevant Legislation and Competent Authorities

1.1 What is the principal data protection legislation?

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, “Canadian Privacy Statutes”).

PIPEDA governs the inter-provincial and international collection, use, and disclosure of personal information.

PIPEDA also applies to organisations that collect, use, and disclose personal information in the course of a commercial activity which takes place within a province. However, PIPEDA will not apply where a province has enacted legislation that has been deemed to be “substantially similar”. The private sector privacy statutes in Alberta, British Columbia, and Québec have each been deemed “substantially similar” to PIPEDA and, as such, PIPEDA will not apply in those jurisdictions. The health privacy statutes in Ontario, New Brunswick, Newfoundland and Labrador have also been deemed substantially similar. (See the response to question 1.3 for information on health privacy legislation in Canada.)

Manitoba has also enacted a private sector privacy statute, entitled the *Personal Information Protection and Identity Theft Prevention Act*, C.C.S.M. c.P-33.7, but it is not yet in force.

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

Canada has also 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 7.1 for details.)

British Columbia, Saskatchewan, Manitoba and Newfoundland have also each adopted a statutory tort of invasion of privacy. Québec civil law also provides individuals with a similar recourse mechanism for privacy violations.

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.

Federal and provincial broader public sector institutions are also subject to public sector privacy legislation.

1.4 What is the relevant data protection regulatory authority(ies)?

The relevant data protection authorities in respect of Canadian Privacy Statutes are as follows: (i) the Office of the Privacy Commissioner of Canada (“OPC”); (ii) the Office of the Information and Privacy Commissioner of Alberta; (iii) the Office of the Information and Privacy Commissioner for British Columbia (“OIPC BC”); and (iv) the *Commission d’accès à l’information*.

2 Definitions

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

- **“Personal Data”**
“Personal Data” (“Personal Information”) is consistently defined very broadly under Canadian Privacy Statutes as information about an identifiable individual. In essence, 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.
- **“Sensitive Personal Data”**
“Sensitive Personal Data” is not defined under Canadian Privacy Statutes. PIPEDA specifically provides that “any information can be sensitive depending on the context”.
- **“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.

- **“Data Controller”**
“Data Controller” is not expressly defined under Canadian Privacy Statutes. Rather, organisations are “accountable” for personal information in their custody or control (including personal information processed by service providers acting on their behalf).
- **“Data Processor”**
“Data Processor” is not defined under Canadian Privacy Statutes. See description of “Data Controller” above for reference to service providers.
- **“Data Subject”**
“Data Subject” is not defined under Canadian Privacy Statutes.
- *Other key definitions – please specify (e.g., “Pseudonymous Data”, “Direct Personal Data”, “Indirect Personal Data”)*
There are no other key definitions in particular.

3 Key Principles

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

- **Transparency**
There are both notice and openness/transparency requirements under Canadian Privacy Statutes.
With respect to notice, while the specific form and substance varies across Canadian Privacy Statutes, organisations are generally required to identify the purposes for which personal information is collected at or before the time the information is collected.
Under the openness and transparency principle under Canadian Privacy Statutes, an organisation must make readily available to individuals specific information about its policies and practices relating to the management of personal information.
- **Lawful basis for processing**
In general, consent is required under Canadian Privacy Statutes for the collection, use and disclosure of personal information (subject to limited exceptions).
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).
- **Purpose limitation**
See the response to the sections on “Data minimisation” and “Proportionality” below.
- **Data minimisation**
Canadian Privacy Statutes require that the collection 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. In addition, 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.
- **Proportionality**
Canadian Privacy Statutes 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.
- **Retention**
Each of the Canadian Privacy Statutes contains a general obligation for organisations to only retain personal information for as long as necessary to fulfil the purposes for which it was collected, subject to a valid legal requirement.

- *Other key principles – please specify*

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.

Canadian Privacy Statutes contain obligations for organisations to ensure that personal information in their 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 is related or is likely to be disclosed to another organisation.

4 Individual Rights

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

- **Access to data**
Under Canadian Privacy Statutes, upon request (and subject to limited exemptions), an individual must be informed of the existence, use, and disclosure of his or her personal information, and must be given access to that information.
The exemptions vary among the statutes and need to be carefully considered in providing the right of access to individuals. Examples of the statutory exemptions include, but are not limited to, circumstances where the disclosure might reveal information subject to solicitor-client privilege, confidential commercial information, information that could threaten the life or security of another individual and information generated in a formal dispute resolution process.
- **Correction and deletion**
Canadian Privacy Statutes 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 in the information, as necessary.
- **Objection to processing**
Under Canadian Privacy Statutes, 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.
- **Objection to marketing**
Consent (either express or implied) is required for the collection, use or disclosure of personal information for marketing purposes. As such, individuals must be able to withdraw their consent to the use of their personal information for marketing purposes. (See also the response to question 7.1.)
- **Complaint to relevant data protection authority(ies)**
Under Canadian Privacy Statutes, individuals have a right to make a complaint to the relevant data protection authority. Individuals must also be able to address a challenge concerning compliance with Canadian Privacy Statutes with the designated individual accountable for the organisation’s compliance. (See also the response to question 6.1.)
- *Other key rights – please specify*
There are no other key rights in particular.

5 Registration Formalities and Prior Approval

5.1 In what circumstances is registration or notification required to the relevant data protection regulatory authority(ies)? (E.g., general notification requirement, notification required for specific processing activities.)

There are no circumstances in which registration or notification to the relevant data protection regulatory authorities is required. (See the response to question 13.2 for notification requirements in the event of a data breach.)

5.2 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.

5.3 Who must register with/notify the relevant data protection authority(ies)? (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.

5.4 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.

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

This is not applicable.

5.6 What is the fee per registration (if applicable)?

This is not applicable.

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

This is not applicable.

5.8 For what types of processing activities is prior approval required from the data protection regulator?

This is not applicable.

5.9 Describe the procedure for obtaining prior approval, and the applicable timeframe.

This is not applicable.

6 Appointment of a Data Protection Officer

6.1 Is the appointment of a Data Protection Officer mandatory or optional?

PIPEDA, PIPA Alberta and PIPA BC expressly require organisations to appoint an individual responsible for compliance with the obligations under the respective statutes. Such individuals are typically referred to as the Chief Privacy Officer or Privacy Officer, although Canadian Privacy Statutes do not prescribe any particular title.

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

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

6.3 What are the advantages of voluntarily appointing a Data Protection Officer (if applicable)?

This is not applicable.

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

Canadian Privacy Statutes do not specify specific qualifications for the Privacy Officer. In recent guidance entitled *Getting Accountability Right with a Privacy Management Program*, the Canadian privacy regulatory authorities set out expectations with respect to the role of the Privacy Officer, including that the Privacy Officer be sufficiently trained with resources dedicated for that purpose. Practically, it would be expected that a Privacy Officer would 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.

6.5 What are the responsibilities of the Data Protection Officer, as required by law or typical in practice?

The Privacy Officer is responsible under Canadian Privacy Statutes for ensuring compliance with applicable privacy law.

In addition, there has been considerable regulatory guidance on specific requirements of the role of the Privacy Officer. Depending on the type and size of the organisation, Canadian privacy regulatory authorities expect the Privacy Officer to, among other things: design, establish and oversee a privacy management programme (including all training, monitoring, documentation, auditing, reporting and evaluation); establish and implement privacy programme controls and assess/revise programme controls as required; be involved in the review and approval process of new initiatives, services and programmes involving personal information; be fundamental to the applicable business decision-making processes of the organisation related to personal information processing; intervene on privacy issues relating to any of the organisation's operations; and represent the organisation in the event of complaints or investigations.

6.6 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 Marketing and Cookies

7.1 Please describe any legislative restrictions on the sending of marketing communications by post, telephone, email, or SMS text message. (E.g., requirement to obtain prior opt-in consent or to provide a simple and free means of opt-out.)

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

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, telemarketing and the use of automatic dialling-announcing devices. See the response to question 7.3 below.

The sending of email and SMS text messages are 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.

7.2 Is 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 1 July 2014. The CRTC has been actively enforcing CASL, and has completed dozens of investigations over the past two years.

7.3 Are companies required to screen against any "do not contact" list or registry?

With respect to telemarketing, under Canada's Do-Not-Call List Rules ("DNCL Rules"), an individual may register their telephone or fax number on the National Do-Not-Call List ("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.

With respect to postal mail, email or SMS marketing, an organisation must maintain its own "do not contact" list.

7.4 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 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 is the agency primarily responsible for regulatory enforcement of the Unsolicited Telecommunications Rules. 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. 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).

7.5 What types of cookies require explicit opt-in consent, as mandated by law or binding guidance issued by the relevant data protection authority(ies)?

There are no specific requirements with respect to cookies under Canadian Privacy Statutes. To the extent that cookies are deemed to process personal information, the full requirements under Canadian Privacy Statutes would apply. (See the response to question 7.6 below for Canadian privacy regulatory authority expectations with respect to cookies and online behavioural advertising.)

CASL sets out an express consent regime for the installation of "computer programmes" and deems cookies to be a type of computer program. CASL provides that a person is considered to expressly consent to the installation of a cookie when the person's conduct is such that it is reasonable to believe that they consent to the cookie's installation.

7.6 For what types of cookies is implied consent acceptable, under relevant national legislation or binding guidance issued by the relevant data protection authority(ies)?

In general, under Canadian Privacy Statutes, implied consent can be relied upon for the collection and use of personal information by cookies to the extent that the personal information involved is non-sensitive in nature.

The OPC has released guidance entitled *Privacy and Online Behavioural Advertising*. In this guidance, the OPC states that

implied (or opt-out) consent is reasonable for the purposes of online behavioural advertising providing 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.

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

Yes. The OPC has issued multiple decisions on cookies, including cookies in the context of online behavioural advertising.

7.8 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, 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 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.

8 Restrictions on International Data Transfers

8.1 Please describe any restrictions on the transfer of personal data abroad.

Under Canadian Privacy Statutes, organisations are responsible for personal information in their custody or control, including personal information transferred to a third party for processing. In general, Canadian Privacy Statutes permit the transfer of personal information without consent for data management purposes/processing purposes where the transferring organisation remains in control of the personal information in the custody of the third party service provider (i.e., to an organisation that would provide data management and processing services, on behalf of the transferring organisation).

8.2 Please describe the mechanisms companies typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions.

Typically, companies enter into an agreement when transferring data outside of Canada for processing purposes in order to ensure that the data transferred is afforded an equivalent level of protection to that under Canadian Privacy Statutes. Depending on the size

and context of the data transfer arrangement in question, there are a number of measures that companies would take to establish an appropriate vendor management framework, including: (i) due diligence, in particular with respect to security safeguards; (ii) contractual arrangements; (iii) appropriate notice to employees or consumers; and (iv) appropriate monitoring of the service provider arrangement.

8.3 Do transfers of personal data abroad require registration/notification or prior approval from the relevant data protection authority(ies)? Describe which mechanisms require approval or notification, what those steps involve, and how long they take.

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

9 Whistle-blower Hotlines

9.1 What is the permitted scope of corporate whistle-blower hotlines under applicable law or binding guidance issued by the relevant data protection authority(ies)? (E.g., restrictions on the scope of issues that may be reported, the persons who may submit a report, the persons whom a report may concern.)

There are no restrictions on the scope of corporate whistle-blower hotlines under Canadian Privacy Statutes. However, assuming that the calls will be recorded, Canadian Privacy Statutes will apply, as the recording of voice communications is considered a collection of personal information. Even if a caller does not provide his or her name, Canadian Privacy Statutes would likely apply as there may be other personal information provided during the call either through the content of the information provided by the caller or merely through the voice of the caller (accent, gender, ethnic origin, age, tone, etc.).

In essence, under Canadian Privacy Statutes, Canadian privacy regulatory authorities have stated that, at the beginning of the call, organisations must provide clear notice to individuals that the call is being recorded and the purposes for the recording. Canadian privacy regulatory authorities have also stated that in the event that the individual objects to the call recording, the organisation must provide an alternative method of communicating (i.e., not record the call or correspond online).

Organisations that are conducting the call recording must also ensure that they comply with the other requirements in Canadian Privacy Statutes with respect to the way in which they manage the personal information collected from call recordings, such as implementing reasonable safeguards, limiting retention, and providing individuals with access to their own call records.

9.2 Is anonymous reporting strictly prohibited, or strongly discouraged, under applicable law or binding guidance issued by the relevant data protection authority(ies)? If so, how do companies typically address this issue?

Anonymous reporting is not strictly prohibited or discouraged under Canadian Privacy Statutes.

9.3 Do corporate whistle-blower hotlines require separate registration/notification or prior approval from the relevant data protection authority(ies)? Please explain the process, how long it typically takes, and any available exemptions.

Corporate whistle-blower hotlines do not require separate registration/notification or prior approval from the relevant data protection authorities.

9.4 Do corporate whistle-blower hotlines require a separate privacy notice?

No. Other than those as set out in the response to question 9.1, a separate privacy notice is not required.

9.5 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 whistle-blower hotlines under Canadian Privacy Statutes.

10 CCTV and Employee Monitoring

10.1 Does the use of CCTV require separate registration/notification or prior approval from the relevant data protection authority(ies)?

No. The use of CCTV does not require separate registration/notification or prior approval from the relevant data protection authorities.

10.2 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:

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

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

Yes. Consent (either express or implied, where permitted) is generally required for employee monitoring or surveillance. Although the specific requirements vary under Canadian Privacy Statutes, in the employment context, implied consent for the collection and use of employee personal information via monitoring would generally be appropriate when: (i) the employee personal information being collected is not sensitive; and (ii) the purpose of

the video surveillance has been explained so that employees would reasonably expect that their information will be used for those purposes.

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.

10.4 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 video surveillance under Canadian Privacy Statutes.

10.5 Does employee monitoring require separate registration/notification or prior approval from the relevant data protection authority(ies)?

Employee monitoring does not require separate registration/notification or prior approval from the relevant data protection authorities.

11 Processing Data in the Cloud

11.1 Is it permitted to process personal data in the cloud? If so, what specific due diligence must be performed, under applicable law or binding guidance issued by the relevant data protection authority(ies)?

Yes. It is permitted to process personal information in the cloud under Canadian Privacy Statutes. The same considerations set out in response to question 8.1 would apply when processing personal information in the cloud.

11.2 What specific contractual obligations must be imposed on a processor providing cloud-based services, under applicable law or binding guidance issued by the relevant data protection authority(ies)?

There are no specific contractual obligations that must be imposed on a processor providing cloud-based services under Canadian Privacy Statutes. There is an evolving set of provisions that Canadian privacy regulatory authorities would expect to be included in contracts with cloud-based or other service providers. These include, among other things: (i) limitations on collection, use, disclosure, access and other processing; (ii) appropriate information security governance; (iii) training and education for service provider employees with access to personal information; (iv) restrictions on sub-contracting; (v) audits; (vi) breach notification protocols; and (vii) data return, anonymisation or destruction requirements.

12 Big Data and Analytics

12.1 Is the utilisation of big data and analytics permitted? If so, what due diligence is required, under applicable law or binding guidance issued by the relevant data protection authority(ies)?

Yes. Assuming that the information in question is personal information, the use of big data and analytics would be permitted

subject to the processes involved in complying with the requirements of Canadian Privacy Statutes. There are no specific requirements with respect to big data or analytics under Canadian Privacy Statutes and there has been no binding guidance on this issue to date. However, the OPC has focused on the privacy challenges inherent in big data processing, and is currently conducting a comprehensive consultation that is considering these issues (see the OPC's discussion paper titled, *A discussion paper exploring potential enhancements to consent under the Personal Information Protection and Electronic Documents Act*).

13 Data Security and Data Breach

13.1 What data security standards (e.g., encryption) are required, under applicable law or binding guidance issued by the relevant data protection authority(ies)?

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.

13.2 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.

Currently, PIPA Alberta is the only private sector privacy statute with a data breach notification requirement. A breach notification requirement was included in recent amendments to PIPEDA, but it is not yet in force.

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 an individual. Notice to the Commissioner must be in writing and include the following information: (i) a description of the circumstances of the loss or unauthorised access or disclosure; (ii) the date on which, or time period during which, the loss or unauthorised access or disclosure occurred; (iii) a description of the personal information involved in the loss or unauthorised access or disclosure; (iv) an assessment of the risk of harm to individuals as a result of the loss or unauthorised access or disclosure; (v) an estimate of the number of individuals to whom there is a real risk of significant harm as a result of the loss or unauthorised access or disclosure; (vi) a description of any steps which the organisation has taken to reduce the risk of harm to individuals; (vii) a description of any steps the organisation has taken to notify individuals of the loss or unauthorised access or disclosure; and (viii) the name of and contact information for a person who can answer, on behalf of the organisation, the Commissioner's questions about the loss or unauthorised access or disclosure.

Once in force, PIPEDA will require that an organisation report to the 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 provided as soon as feasible after the organisation determines that the breach has occurred. The information to be included in the report has yet to be prescribed.

13.3 Is there a legal requirement to report data breaches to individuals? 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.

Under PIPA Alberta, the Commissioner 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: (i) a description of the circumstances of the loss or unauthorised access or disclosure; (ii) the date on which, or time period during which, the loss or unauthorised access or disclosure occurred; (iii) a description of the personal information involved in the loss or unauthorised access or disclosure; (iv) a description of any steps which the organisation has taken to reduce the risk of harm; and (v) contact information for a person who can answer, on behalf of the organisation, questions about the loss or unauthorised access or disclosure.

Once in force, PIPEDA will require an organisation to notify an individual of any breach of security safeguards involving the individual's personal information under the organisation's control 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 yet to be prescribed.

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.

While there are currently no express data breach notification requirements under the remaining Canadian Privacy Statutes, findings and other guidance documents suggest that a duty to notify affected individuals is implicit within the general safeguarding requirements under Canadian Privacy Statutes in circumstances where material harm is reasonably foreseeable, and such notification would serve to protect personal information from further unauthorised access, use or disclosure.

13.4 What are the maximum penalties for security breaches?

Under PIPA Alberta, a failure to notify the Commissioner 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.

Under PIPEDA, failure to comply with the breach notification provisions under PIPEDA will 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.

14 Enforcement and Sanctions

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

Investigatory Power	Civil/Administrative Sanction	Criminal Sanction
Investigations & Orders	<p>The privacy regime in Canada is primarily complaint-based and Canadian privacy regulatory authorities have an express obligation to investigate complaints, and have the authority to self-initiate an investigation.</p> <p>Under PIPEDA, a formal complaint must be investigated and the OPC will issue a Letter of Finding, a report outlining the Findings of the investigation and, if applicable, recommendations for compliance. A Letter of Finding may be made public at the discretion of the OPC. A complainant (but not the organisation subject to the complaint) may appeal to the Federal Court and the Court has broad authority including ordering a correction of the organisation's practices and awarding damages to the complainant, including damages for any "humiliation" that the complainant has suffered.</p> <p>Under PIPA Alberta and PIPA BC, an investigation may be elevated to a formal inquiry by the Commissioner resulting in an order. Organisations are required to comply with the order within a prescribed time period, or apply for judicial review. In both British Columbia and Alberta, 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.</p> <p>Similarly, under the Québec Privacy Act, 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.</p>	N/A
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.	N/A

Investigatory Power	Civil/Administrative Sanction	Criminal Sanction
Monetary Penalties	While penalties are rare in Canada, depending on the jurisdiction in question, Canadian privacy legislation may contain penalties for failure to comply with the obligations set out in the legislation. In Québec, Alberta and British Columbia, there are certain circumstances in which organisations may be subject to 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.	N/A
Compliance Agreements	Under PIPEDA, the OPC may enter into compliance agreements aimed at ensuring organisations comply with PIPEDA, whereby an organisation agrees to take certain actions to bring itself into compliance with PIPEDA.	N/A
Data Sharing Arrangements	The OPC has the express authority under PIPEDA to enter into data sharing arrangements with its provincial or foreign counterparts.	N/A

14.2 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. In particular, the OPC and the provincial privacy regulatory authorities in the provinces of Alberta and British Columbia have been very active in investigating privacy complaints (including complaints into companies such as Facebook and Google), as well as publishing guidance and research on a range of emerging privacy issues. More recently, there has been an increasing trend of Canadian privacy regulatory authorities self-initiating investigations and audits.

In light of the formal arrangements entered into by Canadian privacy regulatory authorities, there have also been joint investigations within Canada and with foreign data protection authorities and the OPC.

15 E-discovery / Disclosure to Foreign Law Enforcement Agencies

15.1 How do companies within your jurisdiction respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?

Although the language varies across the statutes, in general, 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 order that it may be accessed by the courts, law enforcement and national security authorities in those jurisdictions.

15.2 What guidance has the data protection authority(ies) issued?

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

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

16 Trends and Developments

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

Canada has one of the most active privacy regulatory enforcement arenas in the world. In particular, the OPC and the provincial regulatory authorities in the provinces of Ontario, Alberta and British Columbia have collectively been very active in investigating privacy complaints, and publishing guidance and research on a range of emerging privacy issues.

Over the last few years, there has been an increasing trend of Canadian privacy regulatory authorities self-initiating investigations and audits.

In addition, by virtue of a series of formal arrangements entered into by Canadian privacy regulatory authorities and their data protection authority counterparts in foreign jurisdictions, there is an increasing risk that a privacy issue which arises in Canada may also come under privacy regulatory scrutiny in another jurisdiction. In 2016, the OPC conducted a joint investigation with the Australian Privacy Commissioner regarding a security incident involving the compromise of the adult dating website, Ashley Madison. The OPC and provincial regulatory authorities have also been involved in the proactive online privacy sweeps of the Global Privacy Enforcement Network (“GPEN”).

16.2 What “hot topics” are currently a focus for the data protection regulator?

Canadian privacy regulatory authorities are currently focused on the privacy issues associated with digital advertising. As set out in the response to question 7.5, the OPC has issued guidance entitled *Privacy and Online Behavioural Advertising*, has recently released multiple decisions addressing digital advertising and online behavioural advertising (“OBA”), has published a report of research it has conducted on the topic, and is currently conducting investigations regarding the OBA practices of several organisations. The OPC has also been increasingly focused on exploring how the concept of ethics can be integrated into an organisation’s assessment of fair, reasonable and legitimate processing of personal information. Data ethics was expressly considered as part of the OPC’s recent consultation on consent (see response to question 12.1 above), and the OPC recently funded an Information Accountability Foundation project entitled “Big Data Ethics Initiative: Assessment for Canadian Organizations”.

The CRTC has been actively enforcing the commercial electronic message provisions in CASL. The CRTC has issued an administrative monetary penalty of \$1,100,000 to a company for sending commercial electronic messages without consent and which contained an unsubscribe mechanism that did not function properly, entered into four undertakings regarding potential CASL violations that included payments to the CRTC ranging from \$48,000–\$200,000, and one compliance and enforcement decision with an administrative monetary penalty of \$50,000. Furthermore, the enforcement of CASL by the private sector is anticipated when the private right of action under CASL comes into force on July 1, 2017.

**Adam Kardash**

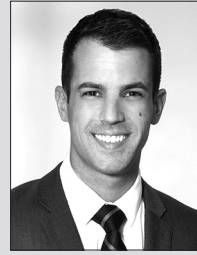
Osler, Hoskin & Harcourt LLP
100 King Street West
1 First Canadian Place
Suite 6200, P.O. Box 50
Toronto ON M5X 1B8
Canada

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 the firm'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>.

**Brandon Kerstens**

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 6744
Email: bkerstens@osler.com
URL: www.osler.com

Brandon is a member of the Commercial group, specialising in Marketing & Distribution and Privacy & Data Management. He is a Certified Information Privacy Professional with the International Association of Privacy Professionals. Brandon has experience on a broad range of privacy and information-management matters, including Canada's anti-spam legislation. His work includes regulatory compliance, conducting privacy and security reviews, drafting privacy policies and service provider agreements, and responding to data breaches.

Brandon also advises on advertising and promotional materials across all media, including compliance issues relating to misleading advertising, contests, games, sweepstakes and consumer-protection issues.

Brandon is the founder and lead of the Osler Pride Network and an Executive Member of the Ontario Bar Association's SOGIC division.

For further information, please visit:
<https://www.osler.com/en/team/brandon-kerstens>.

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 more than 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 on privacy and data management in Canada, providing advice on the increasingly complex rules. The firm's team provides a comprehensive service that includes legal and online privacy information services.

Osler's AccessPrivacy© service offerings help organisations in the public, private and not-for-profit sectors to develop a strategic approach to privacy and information management, supported by sound policies and practices. Our lawyers work closely with our innovative AccessPrivacy© privacy and data management consulting team, which offers clients an integrated suite of consulting, legal and information services.

Other titles in the ICLG series include:

- Alternative Investment Funds
- 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
- Employment & Labour Law
- Enforcement of Foreign Judgments
- Environment & Climate Change Law
- Family Law
- Fintech
- Franchise
- Gambling
- Insurance & Reinsurance
- International 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 Procurement
- Real Estate
- Securitisation
- Shipping Law
- Telecoms, Media & Internet
- Trade Marks
- Vertical Agreements and Dominant Firms



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