ICLG

The International Comparative Legal Guide to:

Data Protection 2015

2nd Edition

A practical cross-border insight into data protection law

Published by Global Legal Group, with contributions from:

A.G. Erotocritou LLC
Adsuar Muñiz Goyco Seda & Pérez-Ochoa, P.S.C.
Affärsadvokaterna i Sverige AB
Brinkhof
Cuatrecasas, Gonçalves Pereira
Dittmar & Indrenius
ECIJA ABOGADOS
ELIG, Attorneys-at-Law
Eversheds
Gilbert + Tobin
Gorodissky & Partners
Herbst Kinsky Rechtsanwälte GmbH
Hogan Lovells BSTL, S.C.
Hunton & Williams LLP
Juridicon Law Firm
Jurisconsul
Lee and Li, Attorneys-at-Law
Matheson
Mori Hamada & Matsumoto
Opice Blum, Bruno, Abrusio
& Vainzof Advogados Associados
Osler, Hoskin & Harcourt LLP
Pachiu & Associates
Pestalozzi
Portolano Cavallo Studio Legale
Subramaniam & Associates (SNA)
Wigley & Company
Wikborg, Rein & Co. Advokatfirma DA

GLG
Global Legal Group

Canada

Adam Kardash

Bridget McIlveen

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) Quebec's *An act respecting the protection of personal information in the private sector*, R.S.Q. ch. P-39.1 ("Quebec 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 Quebec 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. Quebec 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 health care 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 the 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 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 Owner"**

  Data Owner is not defined under Canadian Privacy Statutes.

- **"Data Subject"**

  Data Subject is not defined under Canadian Privacy Statutes.

- **"Pseudonymous Data"**

  Pseudonymous Data is not defined under Canadian Privacy Statutes.

- **"Direct Personal Data"**

  Direct Personal Data is not defined under Canadian Privacy Statutes.

- **"Indirect Personal Data"**

  Indirect Personal Data is not defined under Canadian Privacy Statutes.

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 vary 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**

  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.

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.)

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?

Yes. 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, e-mail, 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 dialing-announcing devices. 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.

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 July 1st, 2015 and a number of investigations are currently underway. The CRTC issued its first Notice of Violation under CASL with a $1.1 million administrative monetary penalty in March, 2015.

7.3 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 Quebec 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 Quebec, 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 Quebec 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).

7.4 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 7.5 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 programs" 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.

7.5 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.

7.6 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.

7.7 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 Quebec, 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 Quebec, 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 Quebec 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).

Under PIPEDA, organisations are expressly required to use contractual or other means to provide a comparable level of protection while the personal information is being processed by a third party.

The Quebec Privacy Act and PIPA Alberta are the only private sector privacy statutes that contain an express reference to transborder data flows. The Quebec Privacy Act requires, among other things, that organisations take reasonable steps to ensure that personal information transferred to service providers outside Quebec will not be used for other purposes and will not be communicated to third parties without consent (except under certain exceptions set out in the statute). PIPA Alberta includes additional notice requirements where the information in question is being transferred outside of Canada, as well as requirements regarding specific information that must be included in applicable privacy policies and procedures about the use of service providers outside Canada.

Certain Canadian federal and provincial public sector privacy statutes and provincial health privacy statutes also contain provisions that impact transborder data flows.

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.

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?; and (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.

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 (although a similar breach notification requirement has been included in proposed amendments to PIPEDA).

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 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.

Proposed amendments to PIPEDA also include a similar breach notification requirement.

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 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.

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.

Proposed amendments to PIPEDA also include a similar breach notification requirement.

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	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. 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. 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 BC 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. Similarly, under the Quebec Privacy Act, an order must be obeyed within a prescribed time period. An individual may appeal to the judge of the Court of Quebec on questions of law or jurisdiction with respect to a final decision.	
Audits	The OPC and the OIPC BC have the express authority to audit the personal information practices of an organisation upon reasonable grounds that the organisation is contravening the Act.	
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 Quebec, Alberta and BC, 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 Quebec, and $100,000 for an offence in Alberta and BC.	
Data Sharing Arrangements	The OPC has the express authority under PIPEDA to enter into data sharing arrangements with its provincial or foreign counterparts.	

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 about 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 Canada 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 that 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. For example, in April 2015, the OPC released its findings on an investigation it initiated following an announcement by Bell Canada, a telecommunications service provider, that it would use customer network usage and account information to enable the serving of targeted ads.

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 increasing risk that a privacy issue that arises in Canada may also come under privacy regulatory scrutiny in another jurisdiction. In 2013, the OPC conducted a joint investigation with the Dutch Data Protection Authority regarding the handling of personal information by the California-based mobile app developer, WhatsApp. 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 response to question 7.5, the OPC has issued guidance on "Privacy and Online Behavioural Advertising", has recently released multiple decisions addressing digital advertising and OBA, and will be publishing a report of research it has conducted on the topic.

The CRTC also recently began enforcement of 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. The CRTC has also entered into an undertaking with the online dating site PlentyOfFish under which the company paid $48,000 for alleged non-compliance with CASL's requirements that unsubscribe mechanisms be able to be 'readily performed' and set out 'clearly and prominently'.

Adam Kardash
Osler, Hoskin & Harcourt LLP
100 King Street West, 1 First Canadian Place
Suite 4600, P.O. Box 50
Toronto ON M5X 1B8
Canada

Tel: +1 416 862 4703
Fax: +1 416 862 6666
Email: akardash@osler.com
URL: www.osler.com

Adam Kardash is an acknowledged Canadian legal industry leader in privacy and data management; he co-leads the Osler's national Privacy and Data Management practice. Widely recognised as an innovator in this fast-moving area of law, Adam also oversees our firm's integrated privacy compliance and data-governance consulting and information service that is complementary to the firm's national privacy and data management practice.

Adam is Special Counsel to the Interactive Advertising Bureau of Canada and counsel to the Digital Advertising Alliance of Canada. Adam has been lead counsel on many of the most significant privacy matters in Canada, including the largest security breach incidents and largest-scale privacy regulatory investigations to date. He advises Fortune 500 clients in their business critical data-protection issues, compliance initiatives and data governance. He regularly represents clients in regulatory investigations and security breaches.

Bridget McIlveen
Osler, Hoskin & Harcourt LLP
100 King Street West, 1 First Canadian Place
Suite 4600, P.O. Box 50
Toronto ON M5X 1B8
Canada

Tel: +1 416 862 4287
Fax: +1 416 862 6666
Email: bmcilveen@osler.com
URL: www.osler.com

Bridget McIlveen is a member of Osler's Privacy and Data Management practice. She advises clients on a broad range of privacy and information-management matters, including drafting privacy policies, responding to security incidents and investigations by privacy regulatory authorities, conducting privacy and security reviews, drafting outsourcing and service provider agreements involving the transfer of personal information, and conducting privacy impact assessments.

She also advises clients on consumer-protection issues associated with carrying on business over the Internet, including compliance with Canada's anti-spam legislation. In addition, she reviews advertising and promotional programmes that involve personal information.

OSLER

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. The firm's lawyers regularly undertake mandates that cross Canada's provincial boundaries as well as international borders.

The firm is known for providing business critical advice and counsel in transformational transactions and litigation for some of the world's largest enterprises. Osler also provides advice and counsel to mid-size and start-up enterprises and on smaller sized matters. The firm is internationally recognised for applying strong legal and business skills to find common-sense business solutions. We are counsel to many of the leading vendors and largest purchasers of technology-related products and services.

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. 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 Recovery & Insolvency
- Corporate Tax
- Data Protection
- Employment & Labour Law
- Environment & Climate Change Law
- Franchise
- Gambling
- Insurance & Reinsurance
- International Arbitration
- Litigation & Dispute Resolution
- Lending & Secured Finance
- Merger Control
- Mining Law
- Oil & Gas Regulation
- Patents
- Pharmaceutical Advertising
- Private Client
- Private Equity
- Product Liability
- Project Finance
- Public Procurement
- Real Estate
- Securitisation
- Shipping Law
- Telecoms, Media & Internet
- Trade Marks

GLG
Global Legal Group

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

www.iclg.co.uk