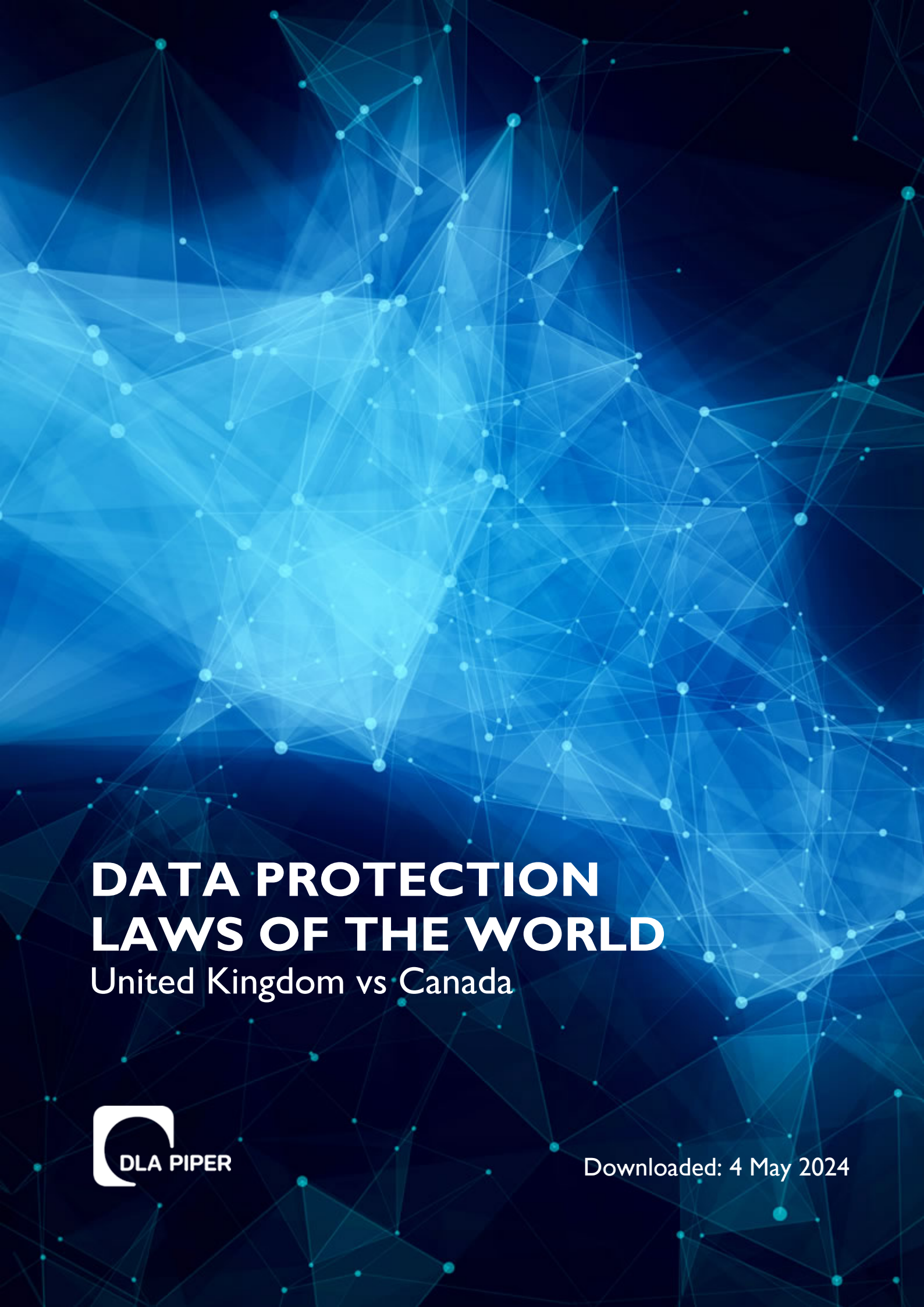

DATA PROTECTION LAWS OF THE WORLD

United Kingdom vs Canada

DLA PIPER

UNITED KINGDOM

Last modified 22 January 2024

LAW

Following the UK’s exit from the European Union, the UK Government has transposed the General Data Protection Regulation (Regulation (EU) 2016/679) into UK national law (thereby creating the **“UK GDPR”**). In so doing, the UK has made a number of technical changes to the GDPR in order account for its status as a national law of the United Kingdom (e.g. to change references to **“Member State”** to **“the United Kingdom”**). These changes were made under the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019. *At this time, all material obligations on controller and processors essentially remain the same under the UK GDPR as under the ‘EU GDPR’.*

The Data Protection Act 2018 (**“DPA”**) remains in place as a national data protection law, and supplements the UK GDPR regime. It deals with matters that were previously permitted derogations and exemptions from the EU GDPR (for example, substantial public interest bases for the processing of special category data, and context-specific exemptions from parts of the GDPR such as data subject rights).

In addition,

- Part 3 of the DPA transposes the Law Enforcement Directive ((EU) 2016/680) into UK law, creating a data protection regime specifically for law enforcement personal data processing;
- Part 4 of the DPA updates the data protection regime for national security processing; and
- Parts 5 and 6 set out the scope of the Information Commissioner's mandate and her enforcement powers, and creates a number of criminal offences relating to personal data processing.

On 8 March 2023, the new ‘Data Protection and Digital Information (No. 2) Bill’ (“the Bill”) was introduced to Parliament following on

CANADA

Last modified 26 January 2023

LAW

In Canada there are 28 federal, provincial and territorial privacy statutes (excluding statutory torts, privacy requirements under other legislation, federal anti-spam legislation, criminal code provisions etc.) that govern the protection of personal information in the private, public and health sectors. Although each statute varies in scope, substantive requirements, remedies and enforcement provisions, they all set out a comprehensive regime for the collection, use and disclosure of personal information.

The summary below focuses on Canada’s private sector privacy statutes:

- Personal Information Protection and Electronic Documents Act ('PIPEDA')
- Personal Information Protection Act (Alberta) ('PIPA Alberta')
- Personal Information Protection Act (British Columbia) ('PIPA BC')
- Act Respecting the Protection of Personal Information in the Private Sector ('Quebec Private Sector Act'), (collectively, 'Canadian Privacy Statutes')

On June 16, 2022, the federal Government introduced Bill C-27, a wide-reaching piece of legislation that is intended to modernize and strengthen privacy protection for Canadian consumers and provide clear rules for private-sector organizations. It is the second attempt to modernize federal private-sector privacy legislation, after a previous proposal died on the order paper in 2021. If adopted, Bill C-27 will replace PIPEDA with legislation specific to consumer privacy rights (the *Consumer Privacy Protection Act*) and electronic documents (the *Electronic Documents Act*). Bill C-27 will also introduce the *Artificial Intelligence and Data Act*, which aims to create rules around the deployment of AI technologies.

Key elements of Bill C-27 include:

- Clarified consent requirements for the collection, use and disclosure of personal information

from the consultation by the Department for Culture, Media and Sport on data protection reforms. The anticipated reforms aim to reduce the compliance burden on organisations. A few of the proposed changes in the Bill include:

- Amendments to certain definitions, such as “identifiable living individual” (impacting the definition of “personal data”) and the meaning of research and statistical purposes;
- Amendments to data protection principles, including the addition of recognised ‘ legitimate interests’ to assist with determining an applicable legal basis;
- Amendments to the conduct of data subject rights, by recognising requests that may be “vexatious or excessive”; and
- Amendments to the obligations of controllers and processors which generally provide more flexibility than the current position, for example with regard to complying with accountability obligations.

It is expected that the Bill will be debated and amended further as it passes through the House of Lords in the first months of 2024, and will likely be enacted through the course of the year.

Territorial Scope

The application of the UK GDPR turns principally on whether an organization is established in the United Kingdom. As under the EU GDPR, an 'establishment' may take a wide variety of forms, and is not limited to a company registered in the United Kingdom.

The UK GDPR also has extra-territorial effect, following the same principles as set out in the EU GDPR. As a result, an organisation that it is not established within the United Kingdom will be subject to the UK GDPR if it processes personal data of data subjects who are in the United Kingdom where the processing activities are related "*to the offering of goods or services*" (Article 3(2)(a)) to such data subjects in the United Kingdom or "*the monitoring of their behaviour*" (Article 3(2)(b)) as far as their behaviour takes place within the United Kingdom.

- Expanded enforcement powers for the Office of the Privacy Commissioner of Canada, including stiff penalties for serious offenses of up ‎ to 5% of annual gross global revenue or CA$25 million
- New rules governing de-identified information
- The creation of a specialized Personal Information and Data Protection Tribunal

C-27 is currently at the committee stage of the legislative process. There has been considerable debate over the Bill, in particular over the proposed *Artificial Intelligence and Data Act.* The final form of the language remains subject to material change.

PIPEDA applies to all of the following:

- Consumer and employee personal information practices of organizations that are deemed to be a ‘federal work, undertaking or business’ (*eg*, banks, telecommunications companies, airlines, railways, and other interprovincial undertakings)
- Organizations who collect, use and disclose personal information in the course of a commercial activity which takes place within a province, unless the province has enacted ‘substantially similar’ legislation (PIPA BC, PIPA Alberta and the Quebec Private Sector Act have been deemed ‘ substantially similar’)
- Inter provincial and international collection, use and disclosure of personal information in connection with commercial activity

PIPA BC, PIPA Alberta and the Quebec Private Sector Act apply to both consumer and employee personal information practices of organizations within BC, Alberta and Quebec, respectively, that are not otherwise governed by PIPEDA.

Quebec recently enacted a major reform of its privacy legislation with the adoption of Bill 64. Bill 64 received Royal Assent on September 22, 2021. A first set of amendments came into force on September 22, 2022, with additional modifications set to come into force on September 22, 2022, while the majority of substantial changes came into force on September 22, 2023. A third, more limited set of amendments will come into force on September 22, 2024. With Bill 64’s changes, Quebec now has in place a sophisticated legal framework for privacy and data protection that resembles the European GDPR in several key areas.

DEFINITIONS

"Personal data" is defined as "any information relating to an identified or identifiable natural person" (Article 4). A low bar is set for "identifiable" – if the natural person can be identified using “all means reasonably likely to be used” (Recital 26) the information is personal data. A name is not necessary either – any identifier will do, such as an identification number, phone number, location data or other factors which may identify that natural person.

Online identifiers are expressly called out in Recital 30, with IP addresses, cookies and RFID tags all listed as examples.

The UK GDPR creates more restrictive rules for the processing of "special categories" (Article 9) of personal data (including data relating to race, religion, sexual life, data pertaining to health, genetics and biometrics) and personal data relating to criminal convictions and offences (Article 10).

The UK GDPR is concerned with the "processing" of personal data. Processing has an extremely wide meaning, and includes any set of operations performed on data, including the mere storage, hosting, consultation or deletion of the data.

Personal data may be processed by either a "controller" or a "processor". The controller is the decision maker, the person who "alone or jointly with others, determines the purposes and means of the processing of personal data" (Article 4). The processor "processes personal data on behalf of the controller", acting on the instructions of the controller. In contrast to the previous law, the GDPR imposes direct obligations on both the controller and the processor, although fewer obligations are imposed on the processor.

The "data subject" is a living, natural person whose personal data are processed by either a controller or a processor.

"Public authority" and "public body" are expressions used in the UK GDPR. The DPA defines them by reference to the definition of "public authority" used in the Freedom of Information Act 2000.

DEFINITIONS

Definition of personal data

‘Personal information’ includes any information about an identifiable individual (business contact information is expressly “carved out” of the definition of ‘personal information’ in some Canadian privacy statutes).

The Quebec Private Sector Act, as modified by Bill 64, has broadened the definition of “personal information” to include any information that allows an individual to be identified indirectly as well as directly. In Quebec, business contact information is included in the definition of “personal information”, however it is considered a less sensitive form of data to which many of the requirements of the Quebec Private Sector Act do not apply.

Definition of sensitive personal data

Not specifically defined in Canadian Privacy Statutes, except for the Quebec Private Sector Act.

The Quebec Private Sector Act, as modified by Bill 64, defines ‎‎“sensitive personal information” as any information ‎that, by virtue of its nature (e.g. biometric or medical), or because of the context in which it is used or communicated, warrants a high expectation of privacy. The Quebec Privacy Act has stricter consent requirements in certain situations for the use and communication of personal information qualified as sensitive.

Definition of anonymized information

The Quebec Private Sector Act, as modified by Bill 64, defines “anonymized information” as information concerning an individual which irreversibly no longer allows such individual to be identified, whether directly or indirectly. Quebec recently adopted a regulation which prescribes certain criteria and procedures which must be followed when anonymizing data.

Definition of de-identified information

The Quebec Private Sector Act, as modified by Bill 64, defines “de-identified information” as any information which no longer allows the concerned individual to be identified directly. “De-

The DPA also clarifies that, where the purpose and means of processing are determined by an enactment of law, then the person on whom the obligation to process the data is imposed by the enactment is the controller.

NATIONAL DATA PROTECTION AUTHORITY

The Information Commissioner (whose functions are discharged through the Information Commissioner's Office **("ICO")**) is the supervisory authority for the UK for the purposes of Article 51 of the UK GDPR. Following Brexit, the ICO no longer has influence or membership in the European Data Protection Board and can no longer be nominated as a lead supervisory authority under the EU GDPR regime. This is reflected in the UK GDPR which omits Chapter 7 (Cooperation and Consistency) of the EU GDPR, on the basis that the UK will not be part of the EU’s cooperation and consistency mechanisms.

The ICO's contact details are:

Wycliffe House
Water Lane
Wilmslow
Cheshire SK9 5AF

T +0303 123 1113 (or +44 1625 545745 if calling from overseas)

F 01625 524510

www.ico.org.uk

REGISTRATION

The UK operates a fee-paying scheme for controllers under the Data Protection (Charges and Information) Regulations 2018, known as the ‘Data Protection Fee’. All controllers have to pay the data protection fee to the ICO annually, unless they are exempt from doing so.

identified” information is still considered to be a form of personal information, to which most of the protections set out in the Quebec Private Sector Act continue to apply.

Definition of biometric information

The Quebec privacy regulator, the *Commission d’accès à l’information* (CAI), defines “biometric information” as information measured from a person’s unique physical, behavioural or biological characteristics. Biometric information is, by definition, sensitive information.

NATIONAL DATA PROTECTION AUTHORITY

Office of the Privacy Commissioner of Canada ('PIPEDA') ‎

Office of the Information and Privacy Commissioner of Alberta ('PIPA Alberta')‎

Office of the Information and Privacy Commissioner for British Columbia ('PIPA ‎BC'), and

Commission d’accès à l’ information du Québec (the “CAI”) ('Quebec Private Sector Act')‎

REGISTRATION

There is no general registration requirement under Canadian Privacy Statutes.

Some registration requirements exist under Quebec privacy laws:

The UK Government has set the fee tiers based on its perception of the risks posed by controllers processing personal data. The amount payable depends upon staff numbers and annual turnover or whether the controller is a public authority, a charity or a small occupational pension scheme. Not every controller must pay a fee – there are exemptions. The maximum fee, for large organisations, is GBP 2,900.

The maximum penalty for a controller who breaks the law by not paying a fee (or not paying the correct fee) is a fine of GBP 4,350 (150% of the top tier fee).

DATA PROTECTION OFFICERS

Under the UK GDPR, each controller or processor is required to appoint a data protection officer if it satisfies one or more of the following tests:

- it is a public authority;
- its core activities consist of processing operations which, by virtue of their nature, scope or purposes, require regular and systemic monitoring of data subjects on a large scale; or
- its core activities consist of processing sensitive personal data on a large scale.

Groups of undertakings are permitted to appoint a single data protection officer with responsibility for multiple legal entities (Article 37(2)), provided that the data protection officer is easily accessible from each establishment (meaning that larger corporate groups may find it difficult in practice to operate with a single data protection officer).

DPOs must have "expert knowledge" (Article 37(5)) of data protection law and practices, though it is possible to outsource the DPO role to a service provider (Article 37 (6)).

Controllers and processors are required to ensure that the DPO is involved "properly and in a timely manner in all issues which relate to the protection of personal data" (Article 38(1)), and the DPO must directly report to the highest management level, must not be told what to do in the exercise of his or her tasks and must not be dismissed or penalised for performing those tasks (Article 38(3)).

The specific tasks of the DPO, set out in the UK GDPR, include (Article 39):

- to inform and advise on compliance with the UK GDPR and other UK data protection laws;

- Personal information agents, defined as “ any person who, on a commercial basis, personally or through a representative, establishes files on other persons and prepares and communicates to third parties credit reports”, must be registered with the CAI
- The use of certain biometric systems and the creation of databases of biometric information must be disclosed to and registered with the CAI

DATA PROTECTION OFFICERS

PIPEDA, PIPA Alberta, and PIPA BC expressly require organizations to appoint an individual responsible for compliance with the obligations under the respective statutes.

The Quebec Private Sector Act, as modified by Bill 64, requires organizations to appoint a person responsible for the protection of personal information, who is in charge of ensuring compliance with privacy laws within the organization. By default, the person with the highest authority within the organization will be the person responsible for the protection of personal information, however this function can be delegated to any person, including a person outside of the organization.

This person’s responsibilities are broadly defined in the law and include:

- Approval of the organization’s privacy policy and ‎practices
- Mandatory privacy impact assessments
- Responding to and reporting security breaches, and
- Responding to and enacting access and ‎ rectification rights

The contact information of the person responsible for the protection of personal information must be published online on the website of the organization.

- to monitor compliance with the law and with the internal policies of the organization including assigning responsibilities, awareness raising and training staff;
- to advise and monitor data protection impact assessments where requested; and
- to cooperate and act as point of contact with the supervisory authority.

COLLECTION & PROCESSING

Data Protection Principles

Controllers are responsible for compliance with a set of core principles which apply to all processing of personal data. Under these principles, personal data must be (Article 5):

- processed lawfully, fairly and in a transparent manner (the "lawfulness, fairness and transparency principle");
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (the "purpose limitation principle");
- adequate, relevant and limited to what is necessary in relation to the purpose(s) (the "data minimization principle");
- accurate and where necessary kept up to date (the "accuracy principle");
- kept in a form which permits identification of data subjects for no longer than is necessary for the purpose(s) for which the data are processed (the "storage limitation principle"); and
- processed in a manner that ensures appropriate security of the personal data, using appropriate technical and organizational measures (the "integrity and confidentiality principle").

The controller is responsible for and must be able to demonstrate compliance with the above principles (the "accountability principle"). Accountability is a core theme of the UK GDPR. Organisations must not only comply with the UK GDPR but also be able to demonstrate compliance perhaps years after a particular decision relating to processing personal data was taken. Record keeping, audit and appropriate governance will all form a key role in achieving accountability.

Legal Basis under Article 6

In order to satisfy the lawfulness principle, each use of personal data must be justified by reference to an

COLLECTION & PROCESSING

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

Subject to certain limited exceptions prescribed in the Acts, consent is required for the ‎collection, use and disclosure of personal information. Depending on the sensitivity of ‎the personal information, consent may need to be presented as opt-in or opt-out. Under the Quebec Private Sector Act, consent must be “ clear, free and informed and be given for specific purposes”: this is generally interpreted as requiring opt-in consent in most situations, however depending on the context and sensitivity of the information, opt-out or implicit consent may, in certain specific situations, be considered valid. Organizations must limit ‎the collection of personal information to that which is necessary to fulfil the identified ‎ purposes and only retain such personal information for as long as necessary to fulfil the ‎purposes for which it was collected.‎

Each of the Canadian Privacy Statutes have both notice and openness/transparency ‎requirements. With respect to notice, organizations are generally required to identify ‎the purposes for which personal information is collected at or before the time the ‎ information is collected. With respect to openness /transparency, generally Canadian ‎Privacy Statutes require organizations make information about their personal ‎information practices readily available.‎

All Canadian Privacy Statutes contain obligations on organizations to ensure personal ‎information in their records is accurate and complete, particularly where the information ‎is used to make a decision about

appropriate basis for processing. The legal bases (also known lawful bases or lawful grounds) under which personal data may be processed are (Article 6(1)):

- with the consent of the data subject (where consent must be "freely given, specific, informed and unambiguous", and must be capable of being withdrawn at any time);
- where necessary for the performance of a contract to which the data subject is party, or to take steps at the request of the data subject prior to entering into a contract;
- where necessary to comply with a legal obligation (under UK law) to which the controller is subject;
- where necessary to protect the vital interests of the data subject or another person (generally recognised as being limited to 'life or death' scenarios, such as medical emergencies);
- where necessary for the performance of a task carried out in the public interest, or in the exercise of official authority vested in the controller; or
- where necessary for the purposes of the legitimate interests of the controller or a third party (which is subject to a balancing test, in which the interests of the controller must not override the interests or fundamental rights and freedoms of the data subject. Note also that this basis cannot be relied upon by a public authority in the performance of its tasks).

Special Categories of Personal Data

Processing of special categories of personal data is prohibited (Article 9), except where one of the following exemptions applies (which, in effect, operate as secondary bases which must be established for the lawful processing of special category data, in addition to an Article 6 basis):

- with the explicit consent of the data subject;
- where necessary for the purposes of carrying out obligations and exercising rights under employment, social security and social protection law or a collective agreement;
- where necessary to protect the vital interests of the data subject or another natural person who is physically or legally incapable of giving consent;
- in limited circumstances by certain not-for-profit bodies;
- where processing relates to the personal data which are manifestly made public by the data subject;

the individual to whom the information relates or if the ‎information is likely to be disclosed to another organization.‎

Each of the Canadian Privacy Statutes also provides individuals with the following:‎

- A right of access to personal information held by an organization, subject to limited ‎ exceptions;
- A right to correct inaccuracies in/update their personal information records; and‎
- A right to withdraw consent to the use or communication of personal information.

In addition to these rights, the Quebec Private Sector Act, as modified by Bill 64, gives individuals the right to have their personal information deindexed. A right to data portability will be coming into force on September 22, 2024.

Finally, organizations must have policies and practices in place that give effect to the ‎requirements of the legislation and organizations must ensure that their employees are ‎made aware of and trained with respect to such policies.‎

- where processing is necessary for the establishment, exercise or defence of legal claims or where courts are acting in their legal capacity;
- where necessary for reasons of substantial public interest on the basis of United Kingdom law, proportionate to the aim pursued and with appropriate safeguards;
- where necessary for preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, provision of health or social care or treatment of the management of health or social care systems and services;
- where necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of health care and of medical products and devices; or
- where necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with restrictions set out in Article 89(1).

Schedule 1 to the DPA supplements the requirements for processing special categories of personal data, and also provides for a number of ‘substantial public interest’ grounds that can be relied upon to process special categories of personal data in specific contexts which are deemed to be in the public interest. Many of these grounds are familiar from the previous UK law, whilst other are new. Important examples include:

- processing required for employment law;
- heath and social care;
- equal opportunity monitoring;
- public interest journalism;
- fraud prevention;
- preventing / detecting unlawful acts (eg money laundering / terrorist financing);
- insurance; and
- occupational pensions.

Criminal convictions and offences data (Article 10)

The processing of criminal conviction or offences data is prohibited by Article 10 of the UK GDPR, except where specifically authorised under relevant member state law. Part 3 of Schedule 1 of the DPA authorises a controller to process criminal conviction or offences data where the processing is necessary for a purpose which meets one of the conditions in Parts 2 of Schedule 1 (this covers the

conditions noted above other than processing for employment law, health and social care), as well as number of other specific conditions:

- consent;
- the protection of a data subject's vital interests; and
- the establishment, exercising or defence of legal rights, the obtaining of legal advice and the conduct of legal proceedings

Appropriate policy and additional safeguards

In any case where a controller wishes to rely on one of the DPA conditions to lawfully process special category, criminal conviction or offences data, the DPA imposes a separate requirement to have an appropriate policy document in place and apply additional safeguards to justify the processing activity. The purpose of the policy document is to set out how the controller intends to comply with each of the data protection principles in Article 5 of the UK GDPR in relation to this more sensitive processing data activity.

Processing for a Secondary Purpose

Increasingly, organisations wish to 're-purpose' personal data - i.e. use data collected for one purpose for a new purpose which was not disclosed to the data subject at the time the data were first collected. This is potentially in conflict with the core principle of purpose limitation; to ensure that the rights of data subjects are protected. The UK GDPR sets out a series of factors that the controller must consider to ascertain whether the new process is compatible with the purposes for which the personal data were initially collected (Article 6(4)). These include:

- any link between the original purpose and the new purpose
- the context in which the data have been collected
- the nature of the personal data, in particular whether special categories of data or data relating to criminal convictions are processed (with the inference being that if they are it will be much harder to form the view that a new purpose is compatible)
- the possible consequences of the new processing for the data subjects
- the existence of appropriate safeguards, which may include encryption or pseudonymisation.

If the controller concludes that the new purpose is incompatible with the original purpose, then the only

bases to justify the new purpose are consent or a legal obligation.

Transparency (Privacy Notices)

The UK GDPR places considerable emphasis on transparency, i.e. the right for a data subject to understand how and why his or her data are used, and what other rights are available to data subjects to control processing. The presentation of granular, yet easily accessible, privacy notices should, therefore, be seen as a cornerstone of UK GDPR compliance.

Various information must be provided by controllers to data subjects in a concise, transparent and easily accessible form, using clear and plain language (Article 12 (1)).

The following information must be provided (Article 13) at the time the data are obtained:

- the identity and contact details of the controller;
- the data protection officer's contact details (if there is one);
- both the purpose for which data will be processed and the legal basis for processing, including, if relevant, the legitimate interests for processing;
- the recipients or categories of recipients of the personal data;
- details of international transfers;
- the period for which personal data will be stored or, if that is not possible, the criteria used to determine this;
- the existence of rights of the data subject including the right to access, rectify, require erasure, restrict processing, object to processing and data portability;
- where applicable, the right to withdraw consent, and the right to complain to supervisory authorities;
- the consequences of failing to provide data necessary to enter into a contract;
- the existence of any automated decision making and profiling and the consequences for the data subject; and
- in addition, where a controller wishes to process existing data for a new purpose, they must inform data subjects of that further processing, providing the above information.

Different requirements apply (Article 14) where information has not been obtained from the data subject.

Rights of the Data Subject

Data subjects enjoy a range of rights to control the processing of their personal data replicating those in the EU GDPR. Controllers must provide information on action taken in response to requests within one calendar month as a default, with a limited right for the controller to extend this period thereby a further two months where the request is onerous.

Right of access (Article 15)

A data subject is entitled to request access to and obtain a copy of his or her personal data, together with prescribed information about the how the data have been used by the controller.

Right to rectify (Article 16)

Data subjects may require inaccurate or incomplete personal data to be corrected or completed without undue delay.

Right to erasure ('right to be forgotten') (Article 17)

Data subjects may request erasure of their personal data. The right is not absolute; it only arises in quite a narrow set of circumstances, notably where the controller no longer needs the data for the purposes for which they were collected or otherwise lawfully processed, or as a corollary of the successful exercise of the objection right, or of the withdrawal of consent.

Right to restriction of processing (Article 18)

Data subjects enjoy a right to restrict processing of their personal data in defined circumstances. These include where the accuracy of the data is contested; where the processing is unlawful; where the data are no longer needed save for legal claims of the data subject, or where the legitimate grounds for processing by the controller are contested.

Right to data portability (Article 20)

Where the processing of personal data is justified either on the basis that the data subject has given his or her consent to processing or where processing is necessary for the performance of a contract, then the data subject has the right to receive or have transmitted to another controller all personal data concerning him or her in a structured, commonly used and machine-readable format (e.g. commonly used file formats recognised by mainstream software applications, such as .xsl).

Right to object (Article 21)

Data subjects have the right to object to processing on the legal basis of the legitimate interests of the data controller or where processing is in the public interest. Controllers will then have to suspend processing of the data until such time as they demonstrate “ compelling legitimate grounds” for processing which override the rights of the data subject.

In addition, data subjects enjoy an unconditional right to object to the processing of personal data for direct marketing purposes at any time.

The right not to be subject to automated decision making, including profiling (Article 22)

Automated decision making (including profiling) "which produces legal effects concerning [the data subject] … or similarly significantly affects him or her" is only permitted where:

- necessary for entering into or performing a contract;
- authorised by UK law; or
- the data subject has given their explicit (i.e. opt-in) consent.

Further, where significant automated decisions are taken on the basis of grounds (a) or (c), the data subject has the right to obtain human intervention, to contest the decision, and to express his or her point of view. Further safeguards for automated decisions that are necessary for entering into or performing a contract or which are authorised by UK law are set out in section 14 of the DPA.

Child's consent to information society services (Article 8)

Article 8(1) of the UK GDPR stipulates that a child may only provide their own consent to processing in respect of information society (primarily, online) services, where that child is over 16 years of age, unless UK law applies a lower age. The DPA reduces the age of consent for these purposes to 13 years for the UK.

TRANSFER

Transfers from the UK

TRANSFER

When an organization transfers personal information to a third-party service provider (*ie*, ‎who acts on behalf of the transferring organization -- although

Transfers of personal data by a controller or a processor to third countries outside of the United Kingdom are only permitted where the conditions laid down in the UK GDPR are met (Article 44).

The United Kingdom Government has the power to make an adequacy decision in respect of a third country under the UK GDPR (Article 45). This power is equivalent to the similar authorities granted to the EC has under the EU GDPR and involves the Secretary of State making a positive determination that the third country provides for adequate level of data protection, following which personal data may be freely transferred to that third country (Article 45(1)). On 21 September 2023, the United Kingdom Government adopted its adequacy decision for the UK Extension for the EU-US Data Privacy Framework, in which an adequate level of protection for personal data transferred the UK to US companies that have joined the framework is ensured in accordance with UK GDPR Art. 45. Currently, the following countries or territories enjoy UK adequacy decisions (these have all essentially been 'rolled over', on a temporary basis, from the EU GDPR): Andorra, Argentina, Canada (with some exceptions), Switzerland, Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, Eastern Republic of Uruguay, United States (if certified under the UK Extension to the EU-US Data Privacy Framework) and New Zealand. The UK is also treating all EU and EEA Member States as adequate jurisdictions, again on a temporary basis. The United Kingdom intends to reassess all these adequacy decisions before the end of 2024. It also has the power to make its own adequacy decisions, and likely time consider new candidates for UK adequacy.

Transfers to third countries are also permitted where **appropriate safeguards** have been provided by the controller or processor and on condition that enforceable data subject rights and effective legal remedies for the data subject are available (Article 46). The list of appropriate safeguards includes, amongst others, binding corporate rules and standard contractual clauses with additional safeguards to guarantee an essentially equivalent level of protection to data subject’s and their personal data[1].

Schedule 21 to the DPA provides that the EU Commission approved standard contractual clauses may continue to be used for transfers under the UK GDPR, until such time as they replaced by clauses issued by the UK Government. Note that the standard contractual clauses carried into UK law are those which were in use

Canadian legislation does not use these terms, the transferring organization would be the “ controller” in GDPR parlance, and the service provider would be a “processor”), the transferring organization ‎remains accountable for the protection of that personal information and ensuring ‎compliance with the applicable legislation, using contractual or other means. In particular, the transferring organization is ‎responsible for ensuring (again, using contractual or other means) that the third party service provider appropriately safeguards ‎the data, and would also be required under the notice and openness/transparency ‎provisions to reference the use of third-party service providers in and outside of Canada ‎in their privacy policies and procedures. ‎

These concepts apply whether the party receiving the personal information is inside or outside Canada. Transferring personal information outside of Canada for storage or processing is generally permitted so long as the requirements discussed above are addressed, and the transferring party notifies individuals that their information may be transferred outside of Canada and may be subject to access by foreign governments, courts, law enforcement or regulatory agencies. This notice is typically provided through the transferring party’s privacy policies.

With respect to the use of foreign service providers, PIPA Alberta specifically requires a ‎transferring organization to include the following information in its privacy policies and ‎procedures:‎

- The countries outside Canada in which the collection, use, disclosure or storage is ‎ occurring or may occur, and
- The purposes for which the third party service provider outside Canada has been ‎ authorized to collect, use or disclose personal information for or on behalf of the ‎ organization

Under PIPA Alberta, specific notice must also be provided at the time of collection or ‎transfer of the personal information and must specify:‎

- The way in which the individual may obtain access to written information about the ‎ organization’s policies and practices with respect to service providers outside ‎ Canada, and
- The name or position name or title of a person who is able to answer on behalf of ‎the

as at the end of 2020. It is expected these will be updated during the course of 2021.

Article 49 of the UK GDPR also includes a list of context specific **derogations**, permitting transfers to third countries where:

- explicit informed consent has been obtained;
- the transfer is necessary for the performance of a contract or the implementation of pre-contractual measures;
- the transfer is necessary for the conclusion or performance of a contract concluded in the interests of the data subject between the controller and another natural or legal person;
- the transfer is necessary for important reasons of public interest;
- the transfer is necessary for the establishment, exercise or defence of legal claims;
- the transfer is necessary in order to protect the vital interests of the data subject where consent cannot be obtained; or
- the transfer is made from a register which according to domestic law is intended to provide information to the public, subject to certain conditions.

There is also a very limited derogation to transfer where no other mechanism is available and the transfer is necessary for the purposes of compelling legitimate interests of the controller which are not overridden by the interests and rights of the data subject; notification to the supervisory authority and the data subject is required if relying on this derogation.

Transfers demanded by courts, tribunals or administrative authorities of countries outside the United Kingdom (Article 48) are only recognised or enforceable (within the United Kingdom) where they are based on an international agreement such as a mutual legal assistance treaty in force between the requesting third country and the United Kingdom; a transfer in response to such requests where there is no other legal basis for transfer will infringe the UK GDPR.

Transfers from the EU to the UK

The UK is now a third country for the purposes of Chapter V of the EU GDPR. .

On 28 June 2021, the EU adopted adequacy decisions in relation to the UK, recognising that the UK offers an

organization the individual’s questions about the collection, use, disclosure or ‎ storage of personal information by service providers outside Canada for or on ‎ behalf of the organization.‎

The Quebec Private Sector Act, as modified by Bill 64, requires all organizations to inform persons that their personal information may be transferred outside of Québec: this is typically done at the time the information is collected. Additionally, before transferring personal information outside of the province of Quebec, organizations conduct data privacy assessments and enact ‎appropriate ‎contractual safeguards to ensure that the information will benefit from adequate protection in the jurisdiction of transfer. These assessments must take into account the sensitivity of the information, the purposes, the level of protection (contractual or otherwise) and the applicable privacy regime of the jurisdiction of transfer. Cross-border transfers may only occur if the organization is satisfied that the information would receive an adequate level of protection. Quebec has decided not to implement a system of ‎adequacy decisions, and ‎ therefore assessments are required prior to any ‎ cross-jurisdiction transfer.

equivalent level of protection of personal data as compared to the EU. This therefore enables personal data to flow freely from the EU to the UK.

For more information, please visit our Transfer - global data transfer methodology website.

1. Following the decision of the Court of Justice of the European Union in the *Data Protection Commissioner v. Facebook and Max Schrems* case (the ‘Schrems II’ case)

SECURITY

The UK GDPR is not prescriptive about specific technical standards or measures. Rather, the UK GDPR adopts a proportionate, context-specific approach to security. Article 32 states that controllers and processors shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk of the processing. In so doing, they must take account of the state of the art, the costs of implementation, and the nature, scope, context and purposes of processing. A 'one size fits all' approach is therefore the antithesis of this requirement.

However the UK GDPR does require controllers and processors to consider the following when assessing what might constitute adequate security:

- the pseudonymisation and encryption of personal data;
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and
- a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

BREACH NOTIFICATION

The UK GDPR contains a general requirement for a personal data breach to be notified by the controller to

SECURITY

Each of the Canadian Privacy Statutes contains safeguarding provisions designed to protect personal information. In essence, these provisions require organizations to take reasonable technical, physical and administrative measures to protect personal information against loss or theft, unauthorized access, disclosure, copying, use, modification or destruction. These laws do not generally mandate specific technical requirements for the safeguarding of personal information.

BREACH NOTIFICATION

the ICO, and for more serious breaches to also be notified to affected data subjects. A "personal data breach" is a wide concept, defined as any "*breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed*" (Article 4).

The controller must notify a breach to the ICO without undue delay, and where feasible, not later than 72 hours after having become aware of it, unless the controller determines that the breach is unlikely to result in a risk to the rights and freedoms of natural persons. When the personal data breach is likely to result in a high risk to natural persons, the controller is also required to notify the affected data subjects without undue delay (Article 34).

Where the breach occurs at the level of the processor, it is required to notify the controller without undue delay upon becoming aware of the breach (Article 33(2)).

The notification to the ICO must include where possible the categories and approximate numbers of individuals and records concerned, the name of the organisation’s data protection officer or other contact, the likely consequences of the breach and the measures taken to mitigate harm (Article 33(3)).

Controllers are also required to keep a record of all data breaches (Article 33(5)) (whether or not notified to the supervisory authority) and permit audits of the record by the ICO.

Breaches in the United Kingdom can be reported to the ICO's dedicated breach helpline during office hours (+44 303 123 1113). Outside of these hours (or where a written notification is preferred) a pro forma may be downloaded and emailed to the ICO.

Currently, PIPEDA, PIPA Alberta, and the Quebec Private Sector Act are the only Canadian Privacy Statutes ‎ with breach notification requirements.‎

In Alberta, an organization having personal information under its control must, without ‎unreasonable delay, provide notice to the Commissioner of any incident involving the ‎loss of or unauthorized access to or disclosure of personal information where a ‎ reasonable person would consider that there exists a real risk of significant harm to an ‎individual as a result. ‎

Notification to the Commissioner must be in writing and include:‎

- A description of the circumstances of the loss or unauthorized access or disclosure
- The date or time period during which the loss or unauthorized access or disclosure ‎ occurred
- A description of the personal information involved in the loss or unauthorized access ‎or disclosure
- An assessment of the risk of harm to individuals as a result of the loss or ‎unauthorized access or disclosure
- An estimate of the number of individuals to whom there is a real risk of significant ‎ harm as a result of the loss or unauthorized access or disclosure
- A description of any steps the organization has taken to reduce the risk of harm to ‎ individuals
- A description of any steps the organization has taken to notify individuals of the loss ‎or unauthorized access or disclosure, and
- The name and contact information for a person who can answer, on behalf of the ‎ organization, the Commissioner’s questions about the loss of unauthorized ‎ access or disclosure

Where an organization suffers a loss of or unauthorized access to or disclosure of ‎personal information as to which the organization is required to provide notice to the ‎Commissioner, the Commissioner may require the organization to notify the individuals ‎ to whom there is a real risk of significant harm. This notification must be given directly ‎to the individual (unless specified otherwise by the Commissioner) and include:‎

- A description of the circumstances of the loss or unauthorized access or disclosure
- The date on which or time period during which the loss or unauthorized access or ‎ disclosure occurred
- A description of the personal information involved in the loss or unauthorized access ‎or disclosure
- A description of any steps the organization has taken to reduce the risk of harm, ‎and
- Contact information for a person who can answer, on behalf of the organization, ‎ questions about the loss or unauthorized access or disclosure

The breach notification provisions under PIPEDA are very similar to the breach ‎notification provisions under PIPA Alberta. The main difference is that PIPEDA requires organizations to notify both the affected individuals and the federal regulator if the breach creates a real risk of significant harm to the individuals (whereas PIPA Alberta requires the initial notice only to the regulator, and then to the individuals if the regulator requires it. In practice, many organizations notify affected Albertans regardless of whether the Alberta Commissioner requires (and the Commissioner typically does require it for most reported breaches in any event). Further, under PIPEDA, organizations must also ‎ keep a record of ALL information security breaches, even those which do not meet the ‎risk threshold of a “real risk of significant harm.”‎

The Quebec Private Sector Act, as modified by Bill 64, introduced a number of new obligations in ‎ connection with “confidentiality incidents”, which are defined as unauthorized access, use, or communication of personal ‎information, or the loss of such information, which were previously absent in Quebec privacy law‎. These include:‎

- A general obligation to ‎prevent, mitigate and remedy security incidents
- The obligation to notify the CAI and the person affected ‎whenever the incident presents a risk of ‎‎“serious ‎ injury.” Factors to consider when evaluating the ‎risk of serious injury include the sensitivity of the ‎information ‎concerned, the anticipated consequences of the ‎use of the information and the likelihood ‎that the information will ‎be used for harmful purposes. Although the Quebec Private Sector Act requires

ENFORCEMENT

Fines

The UK GDPR empowers supervisory authorities to impose fines of up to 4% of annual worldwide turnover, or GBP 17.5 million (whichever is higher).

It is the intention that fines should, where appropriate, be imposed by reference to the revenue of an economic undertaking rather than the revenues of the relevant controller or processor. Recital 150 of the UK GDPR states that 'undertaking' should be understood in accordance with Articles 101 and 102 of the Treaty on the Functioning of the European Union, which prohibit anti-competitive agreements between undertakings and abuse of a dominant position.

Fines are split into two broad categories.

The highest fines (Article 83(5)) of up to GBP 17.5 million or, in the case of an undertaking, up to 4% of total worldwide turnover of the preceding year, whichever is higher, apply to infringement of:

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

The lower category of fines (Article 83(4)) of up to GBP 8.7 million or, in the case of an undertaking, up to 2% of total worldwide turnover of the preceding year, whichever is the higher, apply to infringement of:

organizations to act “promptly” and “with diligence” in response to confidentiality breaches, it does not provide specific timeframes within which such notifications must be made, and

- The obligation on to keep a register of confidentiality ‎incidents, with the CAI having extensive audit rights

Quebec recently adopted regulations further detailing the reporting, notification, and record-keeping obligations of organizations in connection with confidentiality incidents.

ENFORCEMENT

Canadian privacy regulatory authorities have an obligation to investigate complaints, as well as the authority to initiate complaints.

Under PIPEDA, a complaint must be investigated by the Commissioner and a report will be prepared that includes the Commissioner’s findings and recommendations. A complainant (but not the organization subject to the complaint) may apply to the Federal Court for a review of the findings and the court has authority to, among other things, order an organization to correct its practices and award 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. Organizations 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 organization for damages for loss or injury that the individual has suffered as a result of the breach.

In Alberta and BC, a person that commits an offence may be subject to a fine of not more than CA$100,000. Offences include, among other things, collecting, using and disclosing personal information in contravention of the Act (in Alberta only), disposing of personal information to evade an access request, obstructing the commissioner, and failing to comply with an order.

Similarly, under the Quebec Private Sector Act, an order from the CAI must be complied with 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.

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

The ICO is not required to impose fines but must ensure in each case that the sanctions imposed are effective, proportionate and dissuasive (Article 83(1)).

Fines can be imposed in combination with other sanctions. To date, the ICO has issued several fines under GDPR, ranging from GBP 275,000 to GBP 20 million.

Investigative and corrective powers

The ICO also enjoys wide investigative and corrective powers (Article 58) including the power to undertake on-site data protection audits and the power to issue public warnings, reprimands and orders to carry out specific remediation activities.

Right to claim compensation

The UK GDPR makes specific provision for individuals to bring private claims against controllers and processors:

- any person who has suffered "material or non-material damage" as a result of a breach of the UK GDPR has the right to receive compensation (Article 82(1)) from the controller or processor. The inclusion of “non-material” damage means that individuals will be able to claim compensation for distress even where they are not able to prove financial loss.
- data subjects have the right to mandate a consumer protection body to exercise rights and bring claims on their behalf (Article 80).

Individuals also enjoy the right to lodge a complaint with the ICO (Article 77).

All natural and legal persons, including individuals, controllers and processors, have the right to an effective judicial remedy against a decision of the ICO concerning them or for failing to make a decision (Article 78).

Data subjects enjoy the right to an effective legal remedy against a controller or processor (Article 79).

The DPA sets out the specific enforcement powers provided to the ICO pursuant to Article 58 of the UK GDPR, including:

The Quebec Private Sector Act, as modified by Bill 64, introduced a regime of steep fines and administrative penalties in case of non-compliance. The maximum penalties range between CA$5,000 and CA$100,000 in the case of individuals, and up to between CA$15,000$ and CA$25 million or 4% of worldwide turnover for the preceding fiscal year for organizations. This new penalty regime represents a significant change with the previous Quebec regime, under which the maximum penalties were limited to CA $20,000.

There are also statutory privacy torts in various provinces under separate legislation, and Ontario courts have recognized a common-law cause of action for certain privacy torts. In Quebec, a general right to privacy also exists under the *Civil Code of Quebec* and the *Charter of Human Rights and Freedoms*. Organizations may face litigation (including class action litigation) under these statutory and common-law torts, as well as under the general regime of civil liability in Quebec, in addition to any enforcement or claims under Canadian Privacy Statutes.

- information notices – requiring the controller or processor to provide the ICO with information;
- assessment notices – permitting the ICO to carry out an assessment of compliance;
- enforcement notices – requiring the controller or processor to take, or refrain from taking, certain steps; and
- penalty notices – administrative fines.

The ICO has the power to conduct a consensual audit of a controller or a processor, to assess whether that organisation is complying with good practice in respect of its processing of personal data.

Under Schedule 15 of the DPA, the ICO also has powers of entry and inspection. These will be exercised pursuant to judicial warrant and will allow the ICO to enter premises and seize materials.

The DPA creates two new criminal offences in UK law: the re-identification of de-identified personal data without the consent of the controller and the alteration of personal data to prevent disclosure following a subject access request under Article 15 of the GDPR. The DPA retains existing UK criminal law offences, eg offence of unlawfully obtaining personal data.

The DPA requires the ICO to issue guidance on its approach to enforcement, including guidance about the circumstances in which it would consider it appropriate to issue a penalty notice, i.e. administrative fine.

The DPA also requires the ICO to publish statutory codes of practice on direct marketing and data sharing (preserving the position under the previous law).

ELECTRONIC MARKETING

The UK GDPR will apply to most electronic marketing activities, as these will involve some use of personal data (e.g. an email address which includes the recipient's name). The most plausible legal bases for electronic marketing will be consent, or the legitimate interests of the controller (which is expressly referenced as an appropriate basis by Recital 47). Where consent is relied upon, the strict standards for consent under the UK GDPR are to be noted, and marketing consent forms will invariably need to incorporate clearly worded opt-in mechanisms (such as the ticking of an unticked consent box, or the signing of a statement, and not merely the acceptance of terms and conditions, or consent implied from conduct, such as visiting a website).

ELECTRONIC MARKETING

Electronic marketing is governed by both Canadian Privacy Statutes (as discussed ‎above), as well as Canada’s Anti-Spam Legislation (CASL).‎

CASL is a federal statute which prohibits sending, or causing or permitting to be sent, a commercial electronic message (defined broadly to include text, sound, voice, or image messages aimed at encouraging participation in a commercial activity) unless the recipient has provided express or implied consent and the message complies with the prescribed content and unsubscribe requirements (subject to limited exceptions).

Data subjects have an unconditional right to object to (and therefore prevent) any form of direct marketing (including electronic marketing) at any time (Article 21(3)).

Specific rules on electronic marketing (including circumstances in which consent must be obtained) are found in the Privacy and Electronic Communications Regulations 2003 (as amended) (**“PEC Regulations”**). The PEC Regulations are derived from European Union Directive 2002/58/EC (ePrivacy Directive), which have been retained in UK law post-Brexit.

The PEC Regulations prohibit the use of automated calling systems without the consent of the recipient. The PEC Regulations also prohibit unsolicited electronic communications (ie by email or SMS text) for direct marketing purposes without prior consent from the consumer unless:

- the consumer has provided their relevant contact details in the course of purchasing a product or service from the person proposing to undertake the marketing
- the marketing relates to offering a similar product or service, and
- the consumer was given a means to readily 'opt out' of use for direct marketing purposes both at the original point where their details were collected and in each subsequent marketing communication.

Each direct marketing communication must not disguise or conceal the identity of the sender and include the 'unsubscribe' feature referred to above.

The restrictions on marketing by email / SMS only applies in relation to individuals and not where marketing to corporate subscribers.

Enforcement of a breach of the PEC Regulations is dealt with by the ICO. The maximum fine for a breach of the PEC Regulations is GBP 500,000, which can be issued against a company or its directors. The ICO regularly issues fines for direct marketing violations, and it is not uncommon for these to be in the hundreds of thousands of pounds range.

What constitutes both permissible express and implied consent is defined in CASL and its regulations. For example, an organization may be able to rely on implied consent when there is an “existing business relationship” with the recipient of the message, based on:

- A purchase by the recipient within the past two years, or
- A contract between the organization and the recipient currently in existence or which ‎ expired within the past two years

CASL also prohibits the installation of a computer program on any other person's ‎computer system, or having installed such a computer program to cause any electronic ‎messages to be sent from that computer system, without express consent, if the ‎ relevant system or sender is located in Canada. In addition, the Act contains anti ‎phishing provisions that prohibit (without express consent) the alteration of transmission ‎data in an electronic message such that the message is delivered to a destination other ‎than (or in addition to) that specified by the sender.‎

CASL also introduced amendments to PIPEDA that restrict 'address harvesting', or the ‎unauthorized collection of email addresses through automated means (i. e., using a ‎computer program designed to generate or search for, and collect, email addresses) ‎without consent. The use of an individual’ s email address collected through address ‎ harvesting also is restricted.‎

The 'Competition Act' was also amended to make it an offence to provide false or ‎misleading representations in the sender information, subject matter information, or ‎content of an electronic message. ‎

CASL contains potentially stiff penalties, including administrative penalties of up to ‎CA$1 million per violation for individuals and CA$10 million for corporations (subject to a ‎due diligence defense). CASL also sets forth a private right of action permitting ‎individuals to bring a civil action for alleged violations of CASL (CA$200 for each ‎ contravention up to a maximum of CA$1 million each day for a violation of the ‎provisions addressing unsolicited electronic messages). However, the private

ONLINE PRIVACY

The PEC Regulations (as amended) deal with the collection of location and traffic data by public electronic communications services providers ("**CSPs**") and use of cookies (and similar technologies).

Traffic Data

Traffic Data held by a CSP must be erased or anonymised when it is no longer necessary for the purpose of the transmission of a communication.

However, Traffic Data can be retained if:

- it is being used to provide a value added service, and
- consent has been given for the retention of the Traffic Data.

Traffic Data can also be processed by a CSP to the extent necessary for:

- the management of billing or traffic
- dealing with customer enquiries
- the prevention of fraud, or
- the provision of a value added service.

Cookie Compliance

The use and storage of cookies and similar technologies requires:

- clear and comprehensive information, and
- consent of the website user.

The ICO released comprehensive guidance on the use of cookies and similar technologies in 2019. In line with the standard for ‘GDPR like’ consent under the PEC Regulations, this guidance significantly raised the bar in terms of the ICO’s expectations for cookie consent collection. It is now clear that the ICO expects consent to be collected on a clear opt-in basis – implied consent (such as the continued browsing of a website after being shown a cookie banner) is no longer sufficient. Instead, cookie consent modules that given users granular choices about cookie selection (typically on a ‘by purpose’ basis) are becoming the norm in order to align with the guidance.

Consent is not required for cookies that are:

right of ‎action is not yet in force, and there is currently little expectation that it will ever come into force.‎

ONLINE PRIVACY

Online privacy is governed by Canadian Privacy Statutes (discussed above). In ‎general, Canadian privacy regulatory authorities have been active in addressing online ‎privacy concerns.‎

For example, in the context of social media, the OPC has released numerous Reports ‎of Findings addressing issues including:‎

- Default privacy settings
- Social plug-ins
- Identity authentication practices, including data scraping and voiceprint
- The collection, use and disclosure of personal information on social networking sites, including for marketing purposes‎
- The OPC has also released decisions and guidance on privacy in the context of ‎ Mobile Apps

In addition, the OPC has released findings and guidelines related to the use of cookies ‎and online behavioral advertising, including findings indicating that information stored by ‎temporary and persistent cookies is considered to be personal information and ‎therefore subject to PIPEDA. The OPC has adopted the same position with respect to ‎ information collected in connection with online behavioral advertising.‎

In ‘Privacy and Online Behavioral Advertising’, the OPC stated that it may be permissible to use opt-out consent in the context of online behavioral advertising if the following conditions are met:‎

- Individuals are made aware of the purposes for the online behavioral advertising, at ‎or before the time of collection, in a manner that is clear and understandable
- Individuals are informed of the various parties involved in the online behavioral ‎ advertising at or before the time of collection
- Individuals are able to opt-out of the practice and the opt-out takes effect ‎immediately and is persistent

- used for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or
- strictly necessary for the provision of a service requested by the user.

Enforcement of a breach of the PEC Regulations is dealt with by the ICO. The maximum fine for a breach of the PEC Regulations is GBP 500,000, which can be issued against a company or its directors.

- The information collected is non-sensitive in nature (*ie*, not health or financial ‎ information), and
- The information is destroyed or made de-identifiable as soon as possible

The OPC has indicated that online behavioral advertising must not be a condition of ‎service and, as a best practice, should not be used on websites directed at children.‎

Canadian privacy regulatory authorities also consider location data, whether tied to a static location or a mobile device, to be personal information. As such, any collection, use or disclosure of location data requires, among other things, appropriate notice, and consent. Most of the privacy regulatory authority decisions related to location data have arisen with respect to the use of GPS in the employment context.

The Canadian privacy regulatory authorities provide the following test that must be met ‎for the collection of GPS data (and other types of monitoring and surveillance activities):‎

- Is the data demonstrably necessary to meet a specific need?‎
- Will the data likely be effective in meeting that need?‎
- Is the loss of privacy proportional to the benefit gained? ‎
- Are there less privacy-intrusive alternatives to achieve the same objective?‎

Bill 64 introduced several changes to the Quebec Private Sector Act which significantly impact online privacy. Starting September 22, 2023, organizations collecting personal information by offering a product or service with privacy parameters must ensure that the highest privacy settings are enabled by default. Additionally, organizations collecting personal information from persons using tracking, localization or profiling technology (including cookies, trackers, and similar technologies) have the obligation to inform the person in advance of the use of such technologies, and to inform the person of the method for activating such functions: the use of such technologies therefore requires opt-in consent. “ Profiling” is broadly defined as the collection and use of personal information in order to evaluate certain characteristics of a person such as workplace performance, economic or financial situation, health, personal preferences or interest, or behaviour.

Artificial Intelligence

The OPC has also issued guidance on the appropriate use of generative AI systems and has stated that generative AI systems should be developed with the general principles of legality, appropriate purposes, necessity and proportionality, openness and accountability, and:

- In a manner that allows individuals to meaningfully exercise their rights to access their personal information; while
- limiting collection, use and disclosure to only what is needed to fulfill the identified purpose; and
- implementing appropriate safeguards

In addition, the OPC has stated that developers of generative AI models should take steps to ensure that outputs should be as accurate as possible.

KEY CONTACTS

Andrew Dyson
Partner, Global Co-Chair Data Protection, Privacy and Security Group
T +44 (0)113 369 2403
andrew.dyson@dlapiper.com

Ross McKean
Partner
T +44 (0) 20 7796 6077
ross.mckean@dlapiper.com

James Clark
Partner
T +44 113 369 2461
james.clark@dlapiper.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

KEY CONTACTS

Tamara Nielsen
Counsel
T +1 604.643.2952
tamara.nielsen@dlapiper.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.