Global Data Privacy and Cybersecurity Handbook - Canada

| Contents |
| --- |
| To generate table of contents, right-click here and select **Update Field.** |

# What's new?

## Recently Updated Topics

Data Privacy and Cybersecurity in a Transactional Context – updated as of 26 December 2023

Key Cybersecurity Laws and Regulations - updated as of 30 December 2022

New and Material Changes to Data Privacy Laws - updated as of 30 December 2022

Key Enforcement Actions and Priorities - updated as of 30 December 2022

# Key Data Privacy & Cybersecurity Contacts

## Contacts

.

# Key Data Privacy and Cybersecurity Laws

## How are data privacy and cybersecurity laws/regulations implemented?

*Last review date: 26 December 2023*

☒ omnibus – all personal data

☒ sector-specific — e.g., financial institutions, governmental bodies

☒ constitutional

☒ jurisprudence / case law

## What are the key data privacy laws and regulations?

*Last review date: 26 December 2023*

In Canada, data privacy and cybersecurity laws have been enacted at the federal and provincial/territorial level, which apply to private sector entities, public sector entities and "health information custodians." In the following, only the data privacy and cybersecurity laws applicable to private sector entities are covered.

Federal - [Personal Information Protection and Electronic Documents Act](https://laws-lois.justice.gc.ca/eng/acts/P-8.6/), SC 2000, c 5 (PIPEDA)

Alberta - [Personal Information Protection Act](http://www.qp.alberta.ca/1266.cfm?page=P06P5.cfm&amp;amp;amp;leg_type=Acts&amp;amp;amp;isbncln=9780779809530), SA 2003, c P-6.5 (Alberta PIPA)

British Columbia - [Personal Information Protection Act](http://www.bclaws.ca/EPLibraries/bclaws_new/document/ID/freeside/00_03063_01), SBC 2003, c 63 (BC PIPA)

Quebec - [Act respecting the protection of personal information in the private sector](http://www.legisquebec.gouv.qc.ca/en/showdoc/cs/P-39.1), CQLR c P-39.1 (Quebec Act)

## What are the key cybersecurity laws and regulations?

*Last review date: 26 December 2023*

In Canada, the cybersecurity legal landscape is governed by various laws including privacy, anti-spam, criminal liability, and intellectual property:

Generally, federal and provincial privacy laws in Canada regulate the way in which personal information can be collected, used or disclosed. On the federal level, PIPEDA requires an organization to notify affected individuals of any breach of security safeguards involving personal data under its control if it is reasonable in the circumstances to believe that the breach creates a real risk of significant harm to an individual. Similarly, on a provincial level, the Alberta PIPA and recently amended Quebec Act include data breach reporting and notification requirements for private sector organizations.

Canada's anti-spam legislation, 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 (CASL) protects consumers and businesses from spam and other electronic threats. CASL prohibits the following in the course of commercial activity: the alteration of transmission data in an electronic message so that the message is delivered to a destination other than or in addition to that specified by the sender; the installation of a computer program on any other person's computer system without express consent or court order; and the sending of a commercial electronic message to an electronic address in order to induce or aid any of the above prohibitions.

The Criminal Code prohibits the unauthorized use of a computer, the possession of a device to obtain unauthorized use of a computer system or to commit mischief and mischief in relation to computer data.

The Copyright Act includes civil and criminal remedies for the circumvention of technological protection measures and rights management information.

## Are new or material changes to those key data privacy and cybersecurity laws anticipated in the near future?

*Last review date: 26 December 2023*

Yes.

In June 2022, Bill C-27, An Act to enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to make consequential and related amendments to other Acts (Digital Charter Implementation Act, 2022), was introduced to overhaul PIPEDA and modernize the framework for the protection of personal information in the private sector. Bill C-27 is undergoing legislative review in Parliament and if passed, would introduce the following legislative updates:

The new Consumer Privacy Protection Act ("**Act**") would repeal parts of the PIPEDA and replace them with a new legislative regime governing the collection, use, and disclosure of personal information for commercial activity in Canada. This includes updated breach reporting, breach notification, and security safeguard requirements. The Act would also enhance the role of the Office of the Privacy Commissioner of Canada in overseeing compliance with these measures.

The new Personal Information and Data Protection Tribunal Act would create a new administrative tribunal to hear appeals of orders issued by the federal Privacy Commissioner and apply a new administrative monetary penalty regime created under the Consumer Privacy Protection Act.

The Artificial Intelligence and Data Act (AIDA), outlines new measures to regulate international and interprovincial trade and commerce in artificial intelligence systems. AIDA would establish common requirements for the design, development, and use of artificial intelligence systems, including measures to mitigate risks of harm and biased output. AIDA would also prohibit specific practices with data and artificial intelligence systems that may result in serious harm to individuals or their interests.

In June 2022, Bill C-26, An Act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other Acts, was introduced to provide new cybersecurity protections for telecommunications service providers in Canada as well as to ensure that they take certain measures to mitigate or remedy cybersecurity risks. This bill also introduces the Critical Cyber Systems Protection Act (CCSPA), which if passed, would require operators of any "critical cyber system" in Canada, to create a cybersecurity program that meets a number of prescribed safeguards and to notify their respective regulators of their programs. These operators would also have new breach reporting obligations where a cybersecurity incident could interfere with the continuity of a vital system or service.

On 22 September 2021, Quebec's Bill 64,*Act to Modernize Legislative Provisions respecting the Protection of Personal Information* ("Act"), received royal assent. This Act enters into force in phases over a period of three years from the date of assent. This Act increases monetary administrative penalties for violations and creates the following obligations for private sector entities through amendments to the Quebec Act:

Designate a person to be in charge of the protection of personal information within the organization (i.e., privacy officer); mandatory confidentiality incident reporting where there is "risk of serious injury" to an individual and maintenance of a confidentiality incident register

Mandatory privacy impact assessments before transferring personal information outside of Quebec

Inform data subjects when automated decision-making and profiling technologies are being used

Establish and implement governance policies and practices regarding personal information that ensure the protection of such information

Ensure that the parameters of the technological products or services used to collect personal information, by default, provides the highest level of confidentiality, and

Ensure rights of data subjects to data portability.

# Regulators and Enforcement Priorities

## Are there one or more data privacy and/or cybersecurity regulator(s) in the jurisdiction?

*Last review date: 26 December 2023*

Yes.

Federal - [Office of the Privacy Commissioner of Canada](https://www.priv.gc.ca/en/) (OPC)

Alberta - [Information and Privacy Commissioner of Alberta](https://www.oipc.ab.ca/) (Alberta OIPC)

British Columbia - [Information and Privacy Commissioner for British Columbia](https://www.oipc.bc.ca/) (BC OIPC)

Quebec - [Commission d'accès à l'information du Québec](http://www.cai.gouv.qc.ca/english/) (Quebec CAI)

## How active is each of the regulator(s)?

*Last review date: 26 December 2023*

☐ Not very    ☒ Moderately active     ☐ Very active

## What are each of the regulator's anticipated enforcement priorities for the next 12 months?

*Last review date: 26 December 2023*

As the OPC continues to advocate strongly for the enhancement of its enforcement powers through the proposed privacy modernization legislation, it is expected to continue to make full use of the mechanisms already at its disposal, especially investigations into complaints involving businesses subject to PIPEDA to help ensure commercial organizations' digital practices respect the privacy rights of Canadians. If passed, the new federal privacy laws will provide the OPC with strengthened enforcement abilities, including broad order-making powers and authority to assign higher financial penalties for violations.

The OPC launched a secure portal to allow organizations to submit their data breach reports and facilitate future communications regarding the breach. This updated process aims to allow for a more efficient and timely resolution of data breaches by the OPC. The recent OPC investigations into alleged PIPEDA violations, by private sector organizations, have focused on data breaches, the use of audio and video surveillance, location tracking through applications, and obtaining customer consent. In particular, the OPC has focused on breaches resulting from cyber incidents involving compromised credentials (i.e., hacking, malware and phishing scams) and the unauthorized disclosure of personal information. In the near future, the OPC will be completing and implementing a transition plan, for the effective implementation of new federal privacy laws, once they are in effect.

The recent investigations and decisions by the Alberta OIPC, in relation to alleged violations of the Alberta PIPA, focused primarily on data breaches, including unauthorized access to personal information, unauthorized disclosure of personal information, and loss of personal information. The Alberta OPIC, through its investigations, found that the most common cause of breaches is compromised electronic information systems. The recent investigations and decisions by the BC OIPC, in relation to alleged violations of the BC PIPA, focused primarily on the right to access personal information and collection of information through video surveillance systems and facial recognition systems.

Under the amended Quebec Act, organizations must now appoint an internal privacy officer and comply with mandatory incident reporting requirements where there is a "risk of serious injury" to an impacted individual. Effective 22 September 2023, organizations are required to: (i) implement data governance policies; (ii) perform privacy impact assessments before transferring personal information outside of the Province of Quebec; (iii) inform data subjects when automated decision-making and profiling technologies are being used; (iv) comply with enhanced consent requirements; (v) develop an external privacy policy in clear and plain language; (vi) implement "privacy by default" to products and services offered to the public; and (vii) comply with personal information anonymization and destruction requirements. Effective 22 September 2024, organizations must comply with data subject rights to data portability. Under the amended private sector privacy regime, the Quebec CAI is also able to impose significant administrative penalties. It is anticipated that the Quebec CAI will be focused on enforcement activities related to the implementation of the amended and new requirements under the Quebec Act.

# Key Definitions

## Personal data

*Last review date: 26 December 2023*

Personal data generally means information about an identifiable individual. Information will generally be about an "identifiable individual" where there is a serious possibility that an individual could be identified through the use of that information, alone or in combination with other information.

## Sensitive/special personal data (including personal data subject to additional protections/ restrictions/breach notification obligations)

*Last review date: 26 December 2023*

Sensitive data includes:

☒         personal data revealing racial or ethnic origin

☒         personal data revealing political opinions

☒         personal data revealing religious or philosophical belief

☐         personal data revealing trade / professional union or association membership

☒         genetic data

☒         biometric data for the purpose of uniquely identifying a natural person or biometric templates

☒         data concerning health/medical information

☒         data concerning a natural person's sex life or sexual orientation

☒         financial information

☒         government identity card or number information

☒         personal data regarding an individual's criminal convictions or record

☒         passwords

☐        other

## Controller vs Processor

*Last review date: 226 December 2023*

Do the privacy laws distinguish between controllers/owners and processors/agents? Whereby:

The controller/owner is a natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data

The processor/agent is natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller

**Answer:** No

Canadian privacy laws do not define the concepts of controllers and processors. Instead, the principle of accountability dictates that an organization is responsible for personal data that it collects, uses, or discloses. Regardless of whether an organization determines the purposes and means of processing personal data or processes personal data on behalf of another organization, the organization will generally be subject to the same requirements in respect of its collection, use and disclosure of personal data. However, we note that if an organization transfers personal data to a third party for processing, the transferring organization remains responsible for the personal data and must use contractual or other means to provide a comparable level of protection while the data is being processed by a third party.

# Territorial Scope

## What is the territorial reach of the data privacy and cybersecurity laws?

*Last review date: 26 December 2023*

☐        applies to organizations located in the jurisdiction

☐        applies to organizations located outside of the jurisdiction offering goods or services to data subjects in the jurisdiction

☐        applies to organizations located outside of the jurisdiction engaged in the monitoring of the behavior of data subjects located in the jurisdiction

☒        no express territorial scope, but would require some nexus to the jurisdiction

☐        other

# Information Requirements

## What information needs to be included in a privacy notice to data subjects?

*Last review date: 26 December 2023*

☒        the identity and the contact details of the controller and, where applicable, of the controller's representative

☒        the contact details of the data protection officer, where applicable

☒        the purposes of the processing for which the personal data is intended

☐        the legal basis for the processing

☒        the categories of personal data concerned

☐        the source from which the personal data originates and, if applicable, whether it came from publicly accessible sources

☐        the legitimate interests pursued by the controller or by a third party if processing is based on the legitimate interests ground

☒        the recipients or categories of recipients of the personal data, if any

☒        information regarding data transfers to third countries, where applicable, and reference to appropriate or suitable safeguards and the means by which by to obtain a copy of them or where they have been made available

☒        the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period

☒        the existence of data subjects' rights, such as the right to access, rectification, erasure, data portability, etc.

☒        the existence of the right to withdraw consent if processing is based on consent

☐        how the data is held

☒        the security provided to the data

☒        the right to lodge a complaint with a supervisory authority

☒        whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data

☒        if applicable, information regarding automated decision making, including profiling

☐        other

# Legal Bases for Processing of Personal Data

## Is an identified legal basis required in order to collect or process non-sensitive personal data?

*Last review date: 26 December 2023*

Yes.

The following are potential legal bases for processing personal data:

☒        appropriate notice has been provided to or made available to the data subject

☒        the data subject has provided consent to the processing for the identified purposes

☒        the personal data is necessary to perform a contract with the data subject

☒        the personal data is necessary to comply with a legal obligation

☒        the personal data is necessary to protect the vital interests of a natural person

☒        the personal data is necessary for a public interest

☐        the personal data is necessary to fulfil a legitimate interest of the controller or third party (provided that the interest is not overridden by the data subject's privacy interests and the data subject has not made use of his/her right to object)

☒        other

Under PIPEDA, Alberta PIPA, BC PIPA and the Quebec Act, an organization is generally required to obtain consent for any collection, use or disclosure of personal data, subject to limited exceptions that are prescribed (most of which are similar or related to the legal bases listed above).

# Legal Bases for Processing of Sensitive Data

## Is an identified legal basis required in order to collect or process sensitive personal data?

*Last review date: 26 December 2023*

☒ Yes     ☐ No     ☐ No, but additional legal bases are necessary

The following are potential legal bases for processing special categories of personal data:

☐        the data subject has given consent to the processing, where consent is measured to the same standard as non-sensitive personal data

☒        the data subject has given consent to the processing, where consent is measured to a higher standard than for non-sensitive personal data (for example, additional requirement for consent to be "explicit")

☒        processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law

☒        processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent

☐        processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and further conditions

☐        processing relates to personal data which are manifestly made public by the data subject

☐        processing is necessary for the establishment, exercise or defense of legal claims

☐        processing is necessary for reasons of substantial public interest

☐        processing is necessary for the purposes of medicine, the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services

☐        processing is necessary for reasons of public interest in the area of public health

☐        processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes

☒        other

Under PIPEDA, Alberta PIPA, BC PIPA and the Quebec Act, an organization is generally required to obtain consent for any collection, use or disclosure of personal data, subject to limited exceptions that are prescribed (most of which are similar or related to the legal bases listed above).

On 31 October 2023, the Quebec CAI released the final version of its consent guidelines under the Quebec Act, which elaborate on the criteria for validly obtained consent under the Quebec Act.

In May 2022, the OPC issued an [interpretation bulletin](https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-compliance-help/pipeda-interpretation-bulletins/interpretations_10_sensible/), summarizing the general principles on the interpretation of sensitive information under PIPEDA from recent OPC decisions and case law.

In August 2021, the OPC updated several guidance documents to inform organizations on the interpretation of sensitive information under PIPEDA as well as to set out the types of information that will be considered sensitive and require a higher degree of protection.

In March 2021, the Minister of Innovation, Science and Industry issued updated *Guidelines on the National Security Review of Investments*. The updated guidelines outline new and existing factors that the Canadian government will consider in assessing investments for potential national security concerns under the *Investment Canada Act*. The new factors include state-owned enterprises, sensitive personal data, intangible assets, certain sensitive technologies, and critical minerals.

# Data Processing in the Employment Context

## Is an identified legal basis required in order to collect or process personal data or sensitive personal data in the employment context?

*Last review date: 26 December 2023*

Yes.

The potential legal bases for data processing in the employment context are:

Processing is necessary/reasonably required (depending on the applicable private-sector data privacy and security law) for the purposes of establishing, managing or terminating the employment relationship, and the employee has been provided with appropriate notice

## Can consent be validly obtained in the employment context?

*Last review date: 26 December 2023*

☒        Yes, same as for data subjects outside the employment context.

☐        Yes, but this consent is typically more difficult to establish in an employment context (specify details below)

☐        No

PIPEDA only applies to employee personal data of employees of federally regulated businesses (e.g., banks, airlines, and telecommunications companies). Alberta PIPA, BC PIPA and the Quebec Act apply to employee personal data of employees of non-federally regulated businesses in those provinces. Under PIPEDA, Alberta PIPA and BC PIPA, an organization can generally collect, use and disclose employee personal data without consent if the data is necessary (in the case of PIPEDA) or reasonably required (in the case of Alberta PIPA and BC PIPA) for the purposes of establishing, managing or terminating the employment relationship, and the employee has been provided with appropriate notice. Under the Quebec Act, an organization must generally obtain consent to collect, use or disclose employee personal data, though implied consent (i.e., by providing appropriate notice) can be sufficient if the employee's personal data is not sensitive personal data.

## Has the data privacy regulator issued guidance on use of artificial intelligence, automated decision making or profiling in an employment context – for example, relating to use in employee monitoring or hiring?

*Last review date: 26 December 2023*

☒         Yes / No

If yes, please provide a link.

Yes.

In October 2023, the OPC published a resolution of the Federal, Provincial and Territorial Privacy regulators titled "[Protecting Employee Privacy in the Modern Workplace](https://www.priv.gc.ca/en/about-the-opc/what-we-do/provincial-and-territorial-collaboration/joint-resolutions-with-provinces-and-territories/res_231005_02/)" ("Resolution"). This Resolution calls on employers to respect the principles of reasonableness, necessity, and proportionality when implementing AI tools for the collection or use of employee data. Moreover, the Resolution asks employers to refrain from using AI tools to make significant decisions about an employee's candidacy, employment prospects, performance or any other employment related decision without a human to review the output and process.

# Minors

## Are there special requirements that apply to the collection or processing of personal data from minors?

*Last review date: 26 December 2023*

Yes.

The OPC takes the position that, in all but exceptional circumstances, a minor within the meaning of data privacy laws is a person below the age of 13. As of 22 September 2023, a minor within the meaning of the Quebec Act is a person below the age of 14. The Alberta OIPC and BC OIPC do not set a specific age threshold, but rather consider whether the individual understands the nature and consequences of the exercise of the right or power in question.

## In what circumstances do these special requirements apply?

*Last review date: 26 December 2023*

☒        generally

☐        in the context of information society services (e.g., a commercial website) only if processing is based on consent

☐        in the context of educational services

☐        other

## What are the special requirements that apply to collecting or processing personal data from minors?

*Last review date: 2 December 2022*

☒        consent must be given or authorized by the parent/ guardian of the minor

☐        additional data subject rights are granted to minors (e.g., deletion, access, transparency)

☐        additional data security requirements apply

☐        other

# Data Subject Rights

## Do data subjects have specific privacy rights that must be operationalized?

*Last review date: 26 December 2023*

Yes.

Data subjects have the following data privacy rights, although the specifics of the scope and conditions for each of these vary depending on the circumstances and local law:

☒         right to access the data subject's own personal data

☒         right to rectify/correct the data subject's own personal data where inaccurate or incomplete

☒         right to erasure of personal data

☒         right to restrict data processing

☒         right to data portability (as of September 22, 2024 in Quebec)

☒         right to object to the processing of personal data

☒         right to withdraw consent

☐        other

# Artificial Intelligence, Profiling and Automated Decision Making

## Are there any restrictions or requirements related to creating profiles of data subjects or utilizing automated decision making for decisions related to data subjects, including with respect to artificial intelligence?

*Last review date: 26 December 2023*

Yes.

The restrictions or requirements are as follows:

☐        absolute right not to be subject to a decision based solely on automated decision making, including profiling

☐        qualified right not to be subject to a decision based solely on automated decision making, including profiling – for example, only applicable if the decision produces legal effects concerning them or similarly significantly affects them

☒        right to information / transparency requirement

☐        right to request human review of the automated decision making

☒        other

The OPC has published guidance in which it confirms that profiling or categorization which leads to unfair, unethical or discriminatory treatment contrary to human rights law could be considered an inappropriate data practice under PIPEDA.

Effective 22 September 2023, the amended Quebec Act requires that any organization using personal information to render a decision based exclusively on an automated processing of such information must, at the time of or before the decision, inform the concerned person.

## If such restrictions or requirements exist, are they subject to any exceptions?

*Last review date: 26 December 2023*

Yes.

The exceptions are as follows:

Creating profiles of data subjects or utilizing automated decision making for decisions related to data subjects will generally be permitted where, (i) the activity is carried out in accordance with the general requirements under Canadian private-sector data privacy and security laws (i.e., provide notice, obtain consent, etc.); and (ii) the activity does not result in inferences being made about individuals or groups, with a view to profiling them in ways that could lead to unfair, unethical or discriminatory treatment contrary to human rights law.

## Has the data privacy regulator issued guidance on data privacy and artificial intelligence, automated decision-making or profiling?

*Last review date: 26 December 2023*

[Yes/No]

*If yes, please provide brief details and a link.*

Yes.

In December 2023, the OPC, along with provincial privacy regulators, published guidelines respecting the "[Principles for responsible, trustworthy and privacy-protective generative AI technologies](https://www.priv.gc.ca/en/privacy-topics/technology/artificial-intelligence/gd_principles_ai/)". Therein, the OPC outlined nine data privacy principles organizations are strongly encouraged to consider when implementing or developing generative AI technologies.

In September 2023, Innovation, Science and Economic Development Canada (ISED) published a voluntary code of conduct on the "[Responsible Development and Management of Advanced Generative AI Systems](https://ised-isde.canada.ca/site/ised/en/voluntary-code-conduct-responsible-development-and-management-advanced-generative-ai-systems)" ("**Code**"). Private-sector organizations who voluntarily sign the Code agree to abide by a series of principles which carry specific obligations. For example, abiding by the Accountability principle entails the implementation by signatories of a comprehensive risk management framework proportionate to the nature and risk profile of activities.

## Do other (non-privacy or cybersecurity) laws or regulations impose restrictions on use of artificial intelligence, automated decision-making or profiling?

*Last review date: 26 December 2023*

☒     Yes, laws in force

☐        Draft legislation in progress

☐        Proposal for legislation or regulation at an early stage

☐        Non-binding guidance or principles issued or in progress

☐        No, nothing in force or in progress

***If yes, please provide brief details and a link.***

Currently, there are several Canadian federal and provincial frameworks that apply to the different uses of AI. This includes laws related to consumer protection, criminal conduct, human rights, privacy and tort:

Consumer protection laws at the provincial and territorial levels govern the interactions between businesses and their consumers to ensure fair treatment. These laws regulate misleading terms and conditions, misrepresentation of goods or services, and undue pressure.

Product liability can also be imposed on the designers, manufacturers and retailers of AI products through contractual liability, sale of goods laws, consumer protection laws and tort law.

The federal Criminal Code includes prohibitions against the destruction or alteration of computer data and the direct or indirect fraudulent procurement or use of a computer system or computer password.

Federal and provincial human rights commission can provide redress in cases of discrimination, including discrimination that occurs with automated decision-making systems.

Tort law applies where an individual is harmed because of an AI system operated by another entity with whom there is no contractual or commercial relationship (i.e., intentional tort actions, negligence and strict liability).

# Data Protection Officers

## Is the concept of data protection officer (DPO) recognized in the jurisdiction?

*Last review date: 26 December 2023*

Yes.

## Are there circumstances in which it is mandatory to appoint a DPO or similar position?

*Last review date: 26 December 2023*

Yes.

If yes, under what circumstances?

☐        the processing is carried out by a public authority or body, except for courts acting in their judicial capacity

☐        the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale

☐        the core activities of the controller or the processor consist of processing on a large scale of special categories of data

☐        the organization employs more than a certain number of individuals in the jurisdiction

☒        other

Under Canadian private-sector data privacy and cybersecurity laws, organizations are generally required to designate an individual or individuals who are accountable for the organization's compliance with applicable private-sector data privacy and security laws.

## Where a DPO is appointed, does the DPO have to meet specific requirements?

*Last review date: 26 December 2023*

No.

If yes, what are these requirements?

☐  legal qualifications / experience

☐  other professional qualifications / experience

☐  resident in the jurisdiction

☐  other

# Data Processors

## Are there obligations for controllers to establish controls with respect to data processors?

*Last review date: 26 December 2023*

Yes.

The obligations are as follows:

☒        controllers must conduct due conduct diligence on the processor to ensure it will provide appropriate security and processing of the personal data

☒        controllers must only use processors subject to a written agreement that complies with specific requirements

☐        other

## Are there any direct regulatory or statutory requirements on processors?

*Last review date: 26 December 2023*

Yes.

Regardless of whether an organization determines the purposes and means of processing personal data or processes personal data on behalf of another organization, the organization will generally be subject to the same requirements in respect of its collection, use and disclosure of personal data.

# Notification, Filing, Registration & Approval Requirements

## Are there obligations to notify, submit filings to, register with or obtain approval from local data protection authorities to collect and/or process personal data generally?

*Last review date: 26 December 2023*

Yes.

Under the Quebec Act, every "personal information agent" carrying on an enterprise in Quebec must register with the Quebec CAI by filing an application in accordance with prescribed requirements. Under the Quebec Act, a "personal information agent" is 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 bearing on the character, reputation or solvency of the persons to whom the information contained in such files relates. The Quebec CAI must register an agent who files an application in conformity with the prescribed requirements. Upcoming amendments to the Quebec Act include updated "personal information agent" provisions including a requirement for the agent to notify the Quebec CAI within 30 days of any changes to personal and contact information (e.g., name, address, telephone, etc.) and to establish and implement within its enterprise rules of conduct related to the access, protection and rectification of personal information.

# International Data Transfer

## Are there restrictions on the transfer of personal data to third countries?

*Last review date: 26 December 2023*

Yes.

Alberta PIPA specifically requires organizations to notify individuals if they use a service provider outside Canada to collect and/or process personal data.

The Quebec Act specifically requires organizations to obtain individuals' consent in order to communicate their personal data outside Quebec or give a person outside Quebec the authority to hold, use or communicate the information, though implied consent (i.e., by providing appropriate notice) can be sufficient if the personal data is not sensitive personal data. Effective 22 September 2023, the amended Quebec Act requires organizations to conduct a mandatory privacy impact assessment before transferring personal information outside of Quebec. On 22 September 2023, the Quebec CAI released guidance on conducting a privacy impact assessment pursuant to the Quebec Act, and released a model privacy impact assessment for each organization’s consideration.

Transfers of personal data to third countries are only permissible if there is a legal basis for the processing/transfer and one of the following applies:

☐       approved adequate/whitelisted jurisdictions

☐       to holders of specific certifications or followers of specific code of conduct programs each approved by the relevant data protection and cybersecurity authority (e.g., EU-US Data Privacy Framework)

☒      approved standard contractual clauses

☐       binding corporate rules

☐       derogations, such as consent, contract performance, necessity to establish, exercise or defend legal claims

☒       other solutions

Generally, if an organization transfers personal data to a third party (whether inside or outside of Canada), the organization must use contractual or other means to ensure a comparable level of protection for the data while it is being processed by the third party. An organization must also ensure that the data is not used for purposes other than those for which it is transferred.

# Data Localization/Residency

## Are there data localization / data residency or other types of laws that may require the retention and storage of personal data in the local jurisdiction?

*Last review date: 26 December 2023*

Yes.

☒     Data localization / data residency laws that mandate retention of personal data or a copy thereof in the local jurisdiction (include whether copies or the original data may also be stored outside of the jurisdiction):

☐     Other laws that may require the retention and storage of personal data (including, for example, where such data is part of another type of record or dataset) in the local jurisdiction or otherwise prohibit the transfer or disclosure of the personal data outside of the local jurisdiction:

☐        national security laws

☐        anti-investigatory/blocking statutes that restrict any activity on local territory that aids a foreign government investigation

☐         tax or financial record laws

☐        employment laws

☐        export control laws

☐         other

# Security Requirements

## Do data privacy laws or regulations impose obligations to maintain information security controls to protect personal data from unauthorized access or processing?

*Last review date: 26 December 2023*

Yes.

☒         general obligation to take appropriate / reasonable technical, physical and/or organizational security measures

☒         obligation to take specific security measures e.g., encryption

☐        requirement to undertake third party due diligence (security assessment of third party providers)

☐        other

PIPEDA requires organizations to protect personal information through security safeguards that are appropriate to the sensitivity of the information. The security safeguards must protect personal information against loss or theft, as well as unauthorized access, disclosure, copying, use, or modification. The methods of protection should include physical measures (e.g., locked filing cabinets and restricted access to offices), organizational measures (e.g., security clearances and limiting access on an as needed basis), and technological measures (e.g., use of passwords and encryption).

The Alberta PIPA requires that an organization must protect personal information that is in its custody or under its control by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure, copying, modification, disposal or destruction.

The BC PIPA requires that an organization must protect personal information in its custody or under its control by making reasonable security arrangements to prevent unauthorized access, collection, use, disclosure, copying, modification or disposal or similar risks.

The Quebec Act requires that an organization must take the security measures necessary to ensure the protection of the personal information collected, used, communicated, kept or destroyed and that are reasonable given the sensitivity of the information, the purposes for which it is to be used, the quantity and distribution of the information and the medium on which it is stored.

## Do other laws or regulations impose obligations to protect systems from cyberattack?

*Last review date: 26 December 2023*

☒       public company obligations (e.g., duties to maintain sufficient information security measures or ensure operational resilience to cyberattacks?)

☐       network information security requirements (broader than telecommunications)

☒       health regulatory requirements

☒       financial services requirements

☐       telecommunication requirements

☐       providers of critical infrastructure

☒       other

The Office of the Superintendent of Financial Institutions (OSFI) issued an updated *Technology and Cyber Security Incident Reporting Advisory* document, which supports a coordinated and integrated approach to OSFI’s awareness of, and response to, technology and cybersecurity incidents at Federally Regulated Financial Institutions (FRFIs). OSFI also issued Guideline B-13 – Technology and Cyber Risk Management, effective 1 January 2024, which outlines expectations for the sound management of technology and cyber risk for federally regulated financial institutions (FRFIs). In April 2023, OSFI published the *Intelligence Led Cyber Resilience Test* (I-CRT), a framework for identifying areas of vulnerability to sophisticated cyber-attacks among FRFIs. Currently, OSFI expects systemically important banks and internationally active insurance groups to complete an I-CRT assessment at least once every three years, beginning in 2023.  Consistent with guideline B-13, FRFIs will manage overall testing, while OSFI expects FRFIs to establish measures to respond to vulnerabilities by enhancing resilience against cyber-attacks and disruptions. The Canadian Securities Administrators (CSA) issues cybersecurity-related staff notices, including (i) CSA Staff Notice 11-326 (Cyber Security) to inform issuers, registrants and regulated entities on risks of cybercrime and steps to address these risks; (ii) CSA Staff Notice 33-321 (Cyber Security and Social Media) to inform firms on cybersecurity risks associated with social media use; and (iii) CSA Staff Notice 11-332 (Cyber Security) to advance cyber-security awareness, preparedness and resilience in Canadian capital markets. Organizations regulated by the CSA are expected to conduct a cybersecurity risk assessment annually.

Alberta, Ontario, New Brunswick, Newfoundland and Labrador, Nova Scotia, Northwest Territories and the Yukon have data privacy and cybersecurity laws that require health information custodians to take reasonable measures to protect the security and integrity of personal health information, within their control, against unauthorized use, disclosure, and modification.

## Has there been regulatory activity – including enforcement action, investigations, regulatory guidance or other public statements by the regulator – relating to cybersecurity by the following regulators in the last 12 months?

☒      Data privacy

☐      Securities or public company

☐      network information security

☐      health

☐      financial services

☐      telecommunications

☐      critical infrastructure

☐      other

# Breach Notification Requirements

## Does data privacy or cybersecurity law impose obligations to make notifications about personal data security breaches?

*Last review date: 26 December 2023*

Yes.

In Canada, mandatory private-sector breach notification requirements for breaches of personal data other than personal health data exist both at the federal level under the PIPEDA and at the provincial level under Alberta PIPA and the Quebec Act.

Under PIPEDA, a personal data breach (breach of security safeguards) is generally defined as the loss of, unauthorized access to or unauthorized disclosure of personal data resulting from a breach of an organization's security safeguards that are referred to in PIPEDA or from a failure to establish those safeguards.

Under Alberta PIPA, a personal data breach is generally defined as any incident involving the loss of or unauthorized access to or disclosure of personal data.

The Quebec Act requires mandatory confidentiality incident reporting to the Quebec CAI where there is "risk of serious injury" to an individual and for private sector organizations to maintain a confidentiality incident register.

Under BC PIPA, notification is not required, but is a best practice.

## Controllers/ Owners have to notify:

*Last review date: 26 December 2023*

☒        data protection authorities

Under PIPEDA, an organization must notify the OPC and affected individuals of any breach of security safeguards involving personal data under its control if it is reasonable in the circumstances to believe that the breach creates a real risk of significant harm to an individual. While PIPEDA does not prescribe a specific timeframe for breach notification to the OPC, Section 10.1 (2) of PIPEDA requires that the notification must contain certain prescribed information and must be made in a prescribed form and manner, "as soon as feasible after the organization determines that the breach has occurred."

Under Alberta PIPA, an organization with personal data under its control must provide notice to the Alberta OIPC whenever there is a loss of, unauthorized access to, or disclosure of personal data, such that a reasonable person would consider there to be a real risk of significant harm to an individual. The notification must contain certain prescribed information and must be made in a prescribed form and manner. While Alberta's PIPA does not prescribe a specific timeframe for breach notification to the Alberta OIPC, section 34.1 (1) requires that the organization provide notice "without unreasonable delay."

☐       cybersecurity authorities

☒        affected individuals

Under PIPEDA, an organization must notify affected individuals of any breach of security safeguards involving personal data under its control if it is reasonable in the circumstances to believe that the breach creates a real risk of significant harm to an individual. The notification must contain certain prescribed information and must be made in a prescribed form and manner. While PIPEDA does not prescribe a specific timeframe for breach notification to individuals, Section 10.1 (6) requires that the notification be given "as soon as feasible after the organization determines that the breach has occurred."

Alberta PIPA does not require organizations to automatically notify affected individuals when there is a breach; however, the Alberta OIPC has the power to require organizations to notify affected individuals for whom there is a real risk of significant harm.

Under BC PIPA, notification is not required, but is a best practice.

The Quebec Act requires mandatory confidentiality incident reporting, for "risk of serious injury" to an individual, to the Quebec CAI and to the person whose personal information is impacted by the incident.

☒        other

Under PIPEDA, an organization that notifies an individual of a breach of security safeguards must also notify any other organization or government institution or a part of a government institution of the breach if the notifying organization believes that the other organization or the government institution or part concerned may be able to reduce the risk of harm that could result from it or mitigate that harm, or if any of the prescribed conditions are satisfied. While PIPEDA does not prescribe a specific timeframe for breach notification to such organizations, Section 10.2 (2) requires that the notification "be given as soon as feasible after the organization determines that the breach has occurred."

## Processors/ Agents have to notify:

*Last updated: 26 December 2023*

PIPEDA and Alberta PIPA require an organization to report a breach involving personal data under its control. Therefore, the obligation to report the breach rests with an organization in control of the personal data implicated in the breach. The term control is not defined in PIPEDA or Alberta PIPA. The OPC has published guidance interpreting the requirements under PIPEDA, which suggests that in circumstances where an organization (the "principal organization") has transferred personal data to a third party for processing and a breach occurs while the personal data is with the processor, it is reasonable to interpret the principal organization as having control of the personal data and therefore responsibility for breach reporting in respect of a breach that occurs with the third party processor. However, the OPC acknowledges that business relationships can be very complex and determining who has personal data under its control needs to be assessed on a case-by-case basis.

☐        controller/ owner

☐        data protection authorities

☐        cybersecurity authorities

☐        affected individuals

☒        others

# Sector-specific or Non-personal Data Security Breach Notification Requirements

## Are there any additional sector-specific or non-personal data security breach notification requirements?

*Last review date: 26 December 2023*

Yes.

☒        public company obligations (e.g., to notify security incidents that may materially affect an investor's decision)

☐        cybersecurity authorities

☒        health regulatory requirements (e.g., to notify incidents affecting safety of medical devices)

☒        financial services requirements

☐        telecommunication requirements

☒        providers of critical infrastructure

☐        other

Alberta, Ontario, New Brunswick, Newfoundland and Labrador, Nova Scotia, Northwest Territories and Yukon have each enacted data privacy and cybersecurity laws that apply to "health information custodians" (e.g., hospitals, pharmacies, laboratories, nursing homes, ambulance services, healthcare practitioners, etc.) and include security breach notification requirements. In general, health information privacy laws do not prescribe a specific timeframe for breach notification. Rather, in most of these provinces, health information custodians are required to notify individuals and/or the relevant provincial/territorial regulator, "at the first reasonable opportunity" where personal health data is stolen, lost, disposed of, or disclosed to, or accessed by, unauthorized persons, with the exception of Alberta and the Yukon, where notification must be done "as soon as practicable", and "as soon as reasonably possible", respectively. Organizations that fail to comply with the security breach notification requirements can be subject to fines which vary by province/territory (e.g., in Ontario, organizations may be subject to fines of up to CAD 500,000).

Financial regulators such as the CSA, OSFI, IIROC, and MFDA also require the reporting of incidents. These incident reporting obligations generally pertain to any material systems issues, cybersecurity or technology risks and incidents, security breaches, breaches of client confidentiality or system intrusion. While it has neither passed nor entered into force, federal Bill C-26 would enact the *Critical Cyber Systems Protection Act*, which would impose breach reporting obligations on operators of a “critical cyber system” where a breach or suspected breach could impact the continuity of a vital system or service. Schedule 1 defines a “vital system” as a system including federally regulated systems, such as those provided by banks or telecommunications services providers. Operators of critical cyber systems would have breach reporting obligations towards their respective regulators if Bill C-26 were to pass.

# Cookies and Other Online Tracking Technologies

## Are there specific requirements for the use of cookies and other online tracking technologies?

*Last review date: 26 December 2023*

Yes.

Under Canada's Anti-Spam Law (CASL), an organization can generally rely on implied consent to install cookies, as long as the individual's conduct indicates that they consent to it (e.g., if the person disables cookies in their browser, the organization would not be considered to have consent to install cookies). Under PIPEDA, an organization can generally rely on implied consent to collect and use personal data through cookies so long as the personal data is not sensitive and the collection and use aligns with the reasonable expectations of the individual. The OPC has published guidance on online behavioral advertising and the use of cookies, which sets out the conditions under which implied consent to online behavioral advertising can be considered acceptable. The guidance also generally prohibits the use of certain types of cookies and generally prohibits the tracking of children and tracking on websites aimed at children.

# Direct Marketing

## Are there specific requirements related to use of personal data for direct marketing activities?

*Last review date: 26 December 2023*

Yes.

**☒        email marketing**

☒     prior opt-in consent
☐     opt-out or implied consent
☒prior existing business relationship (and subject to other requirements) with opt-out consent

**☒        telephone marketing**

☐      prior opt-in consent
☒     opt-out or implied consent
☐     prior existing business relationship (and subject to other requirements) with opt-out consent

**☒        SMS/text message marketing**

☒      prior opt-in consent
☐      opt-out or implied consent
☒      prior existing business relationship (and subject to other requirements) with opt-out consent

☐**postal marketing**

☐      prior opt-in consent
☐      opt-out or implied consent
☐      prior existing business relationship (and subject to other requirements) with opt-out consent

**☒**      **online behavioral advertising targeting/social media targeting/ad personalization marketing**

☐      prior opt-in consent
☒     opt-out or implied consent
☐      prior existing business relationship (and subject to other requirements) with opt-out consent

# Accountability and Governance

## Are there accountability and governance requirements?

*Last review date: 26 December 2023*

Yes.

There are accountability and governance requirements to:

☒        take privacy by default and design measures for all processing of personal data

☒        perform and document data protection impact assessments (DPIAs) for high-risk processing:

Under the Quebec Act, organizations are required to conduct privacy impact assessments when communicating personal information outside Quebec or when information systems are created or overhauled.

☐        maintain a record of processing activities

☒        implement appropriate measures to comply with data privacy and cybersecurity

☒        demonstrate compliance with data privacy and cybersecurity

☒        identify a specific individual as the data privacy contact for data subject or data protection authority inquiries

☒        provide training to employees

☒        audit or supervise data processors

☐        appoint a local representative in the jurisdiction (if the controller or processor is not located in the jurisdiction)

☐        other

# Penalties for Non-compliance

## What are the potential penalties / remedies for non-compliance with the key data privacy and cybersecurity laws in the jurisdiction?

*Last review date: 26 December 2023*

There are:

☒        administrative remedies / civil penalties applied by regulators and law enforcement

The OPC, Alberta OIPC, BC OIPC and Quebec CAI have the power to investigate complaints from individuals or initiate investigations on their own accord and publish public reports of findings. The OPC cannot make enforceable orders, but the Alberta OIPC, BC OIPC and Quebec CAI can. The OPC can however, after an investigation, make an application to the Federal Court, which has broad order-making powers. The OPC can also enter into compliance agreements with organizations.

☒        criminal penalties from regulators and law enforcement

PIPEDA: Organizations that commit offenses may be subject to fines of up to CAD 100,000.

**Alberta PIPA**: Organizations that commit offenses may be subject to fines of up to CAD 100,000.

**BC PIPA**: Organizations that commit offenses may be subject to fines of up to CAD 100,000.

**Quebec Act**: Following significant increases to monetary penalties effective September 2023, a failure to comply with the Quebec Act's requirements for the collection, storage, communication or use of personal data may result in a fine of up to a maximum amount of CAD 50,000 (approximately USD 40,000) in the case of a natural person and, in all other cases, CAD 10 million (approximately  USD 8 million) or, if greater, the amount corresponding to 2% of worldwide turnover for the preceding fiscal year.

**CASL**: Organizations that fail to comply with certain direct marketing provisions of CASL may be subject to administrative monetary penalties of up to CAD 10 million (approximately USD 8 million).

☒        private remedies

**PIPEDA**: While PIPEDA does not establish a specific private right of action, failure to comply with PIPEDA may result in civil actions, class actions, or private rights of action. A complainant may also, after filing a complaint with the OPC and after receiving the OPC's report of findings or being notified that the complaint has been discontinued, apply to the Federal Court for a hearing. The Federal Court may, in addition to other remedies, order an organization to correct its practices to comply with PIPEDA or award damages to a complainant, including damages for any humiliation that the complainant has suffered.

**Alberta PIPA**: Where the right of appeal for an order made or conviction issued for a breach of Alberta PIPA has been exhausted, an individual affected by the breach has a cause of action for damages for loss or injury they suffered as a result of the breach or conduct.

**BC PIPA**: Where the right of appeal for an order made or conviction issued for a breach of BC PIPA has been exhausted, an individual affected by the breach has a cause of action for damages for the actual harm they suffered as a result of the breach or conduct.

**Quebec Act**: Failure to comply with the Quebec Act may result in civil actions, class actions, or private rights of action. An individual may appeal a final decision of the Quebec CAI and may also apply for leave to appeal from an interlocutory decision of the regulator. Effective from 22 September 2023, individuals can sue private sector organizations for damages pursuant to a new private right of action provision under the amended Quebec Act or under articles 35 to 40 of the Civil Code of Quebec. If the infringement is intentional or results from gross negligence, the court can also award punitive damages of at least CAD 1,000 (approximately USD 799).

☐        other

## If data subjects have private remedies, what form can these remedies take?

*Last review date:*

☒        individual personal actions

☒        representative actions (e.g., brought by a consumer / data privacy body or the supervisory authority)

☒        class actions

# Surveillance

## Are there separate laws or regulations regarding surveillance and/or technology which could be used for surveillance?

*Last review date: 26 December 2023*

No.

If so, what is regulated:

☐      computer tracking / monitoring technology

☐        optical surveillance devices (e.g., CCTV cameras)

☐        audio surveillance / recording technology

☐        workplace surveillance

☐        facial recognition technology

☐        other biometric recognition technology

☐        other

# Risk Rating

## What is the risk of non-compliant data privacy and cybersecurity practices for private sector organizations in the jurisdiction?

*Last review date: 26 December 2023*

☒        high (e.g., well-established privacy laws and regulations with strict compliance requirements, active regulator)

☒        medium (somewhere in between)

☐        low (e.g., relatively new or no privacy laws, inactive regulator)

# Most Common Compliance Mistakes

## What are the top three most common data privacy and cybersecurity compliance mistakes made by companies doing business in the jurisdiction?

*Last review date: 26 December 2023*

☒         insufficient data subject notice

☐         lack of up-to-date record of processing

☒         insufficient data security or insufficient data security breach response

☐         insufficient agreements with processors

☐         lack of registration with /notification to / approval from the supervisory authority

☐         failure to address cross-border transfer requirements

☐         failure to address data residency requirements

☐         failure to appoint a data protection officer, local representative or similar position

☐         failure to comply with data subject rights requests

☒         lack of legal basis for processing (including invalid consent)

☐         lack of compliance with marketing requirements

☐         non-compliant automated decision making

☐         processing sensitive personal data incorrectly or without sufficient legal basis

☐        other

# Data privacy and cybersecurity in a transactional context

## Has the data privacy authority issued any guidance on data privacy compliance in the context of transactional activity (including, but not limited to, share sales, asset sales, reorganizations or spinouts)?

*Last review date: 26 December 2023*

☐        Yes

☒        No

If yes, please provide a link

## In the context of an asset sale (the sale of a separate business unit as a going concern), does the acquiring entity inherit liability for pre-acquisition data privacy or cybersecurity breaches (connected with the assets that are the subject of the asset sale)?

*Last review date: 26 December 2023*

☐        Yes

☐       No

☒        It depends (for example, on the way the asset sale is structured, and/or the assets being acquired)

☐        Unclear

Generally, the organization that is in control of personal information that is subject to a cyber-security breach or data privacy violations would retain liability and be subject to the applicable fine. Therefore, purchasers must integrate careful review of the target's data protection systems and processes and investigate whether any breaches are ongoing.

## If so, how would any regulatory fines be calculatedxx?

*Last review date: 26 December 2023*

☐        Based on turnover of the entity (or group) that owned the assets at the time of the breach

☐        Based on the value of the transferred assets

☐        Based on the turnover of the entity (or group) that owned the assets at the time the breach is identified (which, if the breach is identified post-acquisition, may be the turnover of the acquiring entity or group)

☐        Based on the turnover of the entity (or group) that owned the assets at the time the fine is imposed (which, if the fine is imposed post-acquisition, may be the turnover of the acquiring entity or group)

☐        Based on a metric other than those outlined above

☒        Unclear

## In the context of a share sale (where the acquiring entity acquires 100% of the shares of a target company), does the acquiring entity inherit liability for pre-acquisition data privacy or cybersecurity breaches (connected with the target company)?

*Last review date: 26 December 2023*

☒        Yes

☐        No

☐        It depends (for example, on the way the share sale is structured)

☐        Unclear

The OPC has emphasized that in the context of a share sale, the acquiring entity inherits liability for pre-acquisition data privacy or cybersecurity breaches. For example, the OPC addressed the inherited liability of pre-acquisition data privacy breaches in PIPEDA Findings #2022-005. There, a global hotel chain ("Purchaser") was held accountable and investigated for failure to mitigate a pre-acquisition cyber-security breach incurred by the target it had acquired.

## If so, how would any regulatory fines be calculated?

*Last review date: 26 December 2023*

☐        Based on the turnover of the target company (or its group) at the time of the breach

☐        Based on the turnover of the target company (or its group) at the time that the breach is identified (which, if the breach is identified post-acquisition, may be the turnover of the acquiring entity or group)

☐        Based on the turnover of the relevant entity (or group) at the time that the fine is imposed (which, if the breach is identified post-acquisition, may be the turnover of the acquiring entity or group)

☐        Based on a metric other than those outlined above#

☐        Unclear