Global Privacy Regulatory Framework and Industry Trends

With many different data protection laws around the globe, all with their own requirements and many with overlapping scope, it can be difficult to know exactly which laws apply to any given organization. In this document, we have provided a high-level overview of the requirements that are common to many data protection laws, and have pointed out where some of these laws diverge from the rest and impose different obligations. In doing so, we hope to assist organizations in determining which laws apply to them and what steps they may need to take in order to achieve global compliance.

I- OVERVIEW OF GLOBAL PRIVACY LAWS

Privacy is a fast-evolving area of law and upcoming regulatory changes should continue to be closely monitored. In the interim, organizations handling personal information can take protective measures to mitigate risk by investing in compliance programs, in robust security systems and by conducting mandatory employee training.

a. Canada

Private sector organizations doing business in Canada will need to take into account the following privacy framework, which is constantly evolving:

(i) Data Protection Laws

- **Federal law**: In Canada, the federal *Personal Information Protection and Electronic Documents Act* ("PIPEDA") sets out ground rules for how private sector federal works, undertakings and businesses collect, use and disclose personal information about individuals.[1] PIPEDA also applies to personal information that organizations collect, use and disclose in the course of their commercial activities, unless such activities are regulated by provincial legislation that has been declared substantially similar to PIPEDA.

- **Provincial laws:** The provinces of British Columbia,[2] Alberta[3] and Quebec[4] have enacted provincial data protection legislation that has been recognized as substantially similar to PIPEDA,[5] and therefore, this legislation operates in place of PIPEDA in those provinces for intra-provincial matters. While these provincial laws regulate the personal information of any private sector

[1] *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5, s. 3. PIPEDA is applicable to organizations carrying on "federal work, undertaking or business" (s. 2 "federal work, undertaking or business"; s. 4(1)(b)) and organizations in provinces and territories where no personal information protection act has been enacted, such as Ontario (i.e. all provinces except Quebec, Alberta and British Columbia).

[2] *Personal Information Protection Act* (British Columbia), S.B.C. 2003, c. 63.

[3] *Personal Information Protection Act* (Alberta), S.A. 2003, c. P-6.5.

[4] *An Act Respecting the Protection of Personal Information in the Private Sector*, R.S.Q. 1993, c. P-39.1.

[5] Under subparagraph 26 (2) (b) of PIPEDA.

organization's customers as well as employees, PIPEDA regulates the personal information of customers and only the personal information federal works' employees (such as telcos and banks).

(ii) Privacy Laws and Torts

Many provinces have additional specific privacy laws, or other more general laws that may include provisions regulating privacy or the security of information. This includes but is not limited to:

- The Civil Code of Quebec, the Quebec *Charter of human rights and freedoms,*[6] the Quebec *An act to establish a legal framework for information technology;*[7] and
- The British Columbia *Privacy Act*.[8]
- In Ontario, a recent tort of intrusion upon seclusion was recognized in 2012 by the Ontario Court of Appeal in *Jones v. Tsige.*[9]

Several federal and provincial sector-specific laws include provisions dealing with the protection of personal information. The federal *Bank Act*,[10] for example, contains provisions regulating the use and disclosure of personal financial information by federally regulated financial institutions. Most provinces have legislation dealing with consumer credit reporting. Provincial laws governing credit unions typically have provisions dealing with the confidentiality of information relating to members' transactions. There is also a large number of provincial acts that contain confidentiality provisions concerning personal information collected by professionals. A few provinces have privacy legislation, which applies to health information that has been declared substantially similar to PIPEDA with respect to health information custodians.[11]

(iii) Mandatory breach notification

With security breaches being on the rise, the requirement to have organizations notify the relevant privacy commissioners and affected individuals upon a security breach taking place is viewed as becoming increasingly important. The first Canadian jurisdiction that has made security breach notification mandatory is Alberta, although in other Canadian jurisdictions, it seems like things are about to change. At the federal level, the mandatory breach notification requirement came into effect in fall 2018.

---

[6] chapter C-12.

[7] chapter C-1.1.

[8] [RSBC 1996] Chapter 373.

[9] 2012 ONCA 32.

[10] (S.C. 1991, c. 46).

[11] See the Ontario *Personal Health Information Protection Act,* S.O. 2004, CHAPTER 3 SCHEDULE A, the New Brunswick *Personal Health Information Privacy and Access Act* (S.N.B. 2009, c. P-7.05) and the Newfoundland and Labrador's Personal Health Information Act, SNL2008 CHAPTER P-7.01. While other provinces and territories have also passed their own health privacy laws, these have not been declared substantially similar to PIPEDA. Therefore in some cases PIPEDA may still apply.

b. Europe

The *General Data Protection Regulation* ("**GDPR**"),[12] which replaced the European Directive 95/46/EC, came into effect in May 25, 2018 and is widely considered the most stringent data protection law in the world. One of the most significant changes brought in by the GDPR is that it is a "regulation," as opposed to a "directive." A regulation applies directly in all European Union ("**EU**") Member States and allows them little discretion in implementation, whereas a directive sets desired results but depends upon Member State implementation, which may lead to a patchwork of national laws. The GDPR aims at harmonizing the various data protection laws across the EU.

The GDPR applies to organizations based in the EU as well as all other organizations that collect and use the personal information of EU residents. This "extra-territoriality" means that organizations that operate in Canada but target their goods or services at EU residents must comply with the requirements of the GDPR. The GDPR provides EU residents with broad rights in relation to their data, and these translate into strict requirements for organizations, such as the right to erasure, also known as the "right to be forgotten", the right to be notified of a security incident involving their personal data within 72 hours of the organization becoming aware of the incident, and the right to data portability, among others. Violations of the requirements of the GDPR carry strict penalties, and non-compliance can cost an organization up to 4% of annual global turnover, or €20 million – whichever is higher.

c. U.S.

There is not currently a comprehensive, nationwide data protection law in the U.S. However, there are sector-specific laws that include privacy protection provisions, such as the *Fair Credit Reporting Act*, the *Children's Online Privacy Protection Act* and the *Telemarketing and Consumer Fraud and Abuse Prevention Act*. These are enforced by the Federal Trade Commission ("**FTC**"), which also enforces the *Federal Trade Commission Act*, which prohibits organizations from engaging in unfair competition and unfair acts or practices that affect commerce. It is on the basis of this Act that the FTC primarily enforces organizations' data protection obligations. Furthermore, most states have their own specific laws outlining breach notification requirements, although the threshold for requiring notification is relatively high and many of these only apply to breaches involving extremely sensitive information, such as social security numbers. In 2018, California passed the non sector-specific *California Consumer Privacy Act*, and since then at least 18 states have introduced their own privacy legislation, although only those in California, Maine and Nevada have been signed into law.

(i) California

The *California Consumer Privacy Act* ("**CCPA**")[13], which will come into effect on January 1, 2020, regulates for-profit organizations (i) doing business in California, (ii) collecting personal information about California households and consumers (essentially defined as California residents) and (iii) that either: have annual gross revenues in excess of U.S. $25 million; buy, receive, sell, or share the personal information of more

[12] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

[13] Ca. Civ. Code §§ 1798.100 - .199

than 50,000 California residents; and/or derive 50% or more of their annual revenues from selling California residents' personal information. Although the notion of "doing business in California" has yet to be interpreted, it is likely that this will apply extraterritorially to organizations that offer products or services in the state, including online.

The CCPA imposes many standard data protection obligations on organizations, such as transparency and access rights, but also provides individuals with rights to deletion and data portability that are similar to those provided for under the GDPR. The CCPA also imposes its own unique obligations, such as the obligation to provide individuals with the right to opt out of having their information sold, and a requirement that organizations provide a clear and conspicuous link on their website's homepage titled "Do Not Sell My Personal Information" leading to a page enabling consumers to opt out of the sale of their personal information. Under the CCPA, a "sale" includes non-monetary compensation.

(ii) Maine

In Maine, *An Act to Protect the Privacy of Online Consumer Information*[14] was the signed into law on June 7, 2019 and will take effect on July 1, 2020. This new law only applies to internet service providers (ISPs) operating in Maine and providing services to individuals who are physically located in Maine. ISPs must adopt adequate data protection safeguards, notify individuals of their rights regarding such information, and obtain opt-in consent to use, disclose or sell customer personal information to third parties, which includes information collected from the customer's use of the Internet, such as their browsing history, geolocation, device identifier and IP address.

(iii) Nevada

Nevada's data protection law[15] came into effect in 2017 but has been amended to include a right for customers to opt-out of the sale of their personal information. The amendments came into effect on October 1, 2019. Nevada's privacy law applies to online businesses, services and operators of internet websites that collect personal information from consumers who reside in Nevada and purposefully conduct their activities toward Nevada, including concluding transactions with a Nevada resident. Nevada's law does not provide individuals with the rights of access, portability, deletion or non-discrimination, but now requires organizations to provide them with the right to opt-out of having their information sold for monetary compensation. In order to give effect to this right, organizations must provide an online mechanism or toll-free phone number that individuals can use to opt-out. This law contains certain exemptions for service providers of the entities that are subject to its requirements and certain financial institutions as well as health-care institutions subject to HIPAA.

[14] LD 946.

[15] SB220/Chapter 603A.

d. Asia (Japan, China)

(i) Japan

In Japan, organizations must comply with Japan's *Act on the Protection of Personal Information* ("**APPI**")[16], which was significantly amended in May 2017. Since being amended, the APPI has an extraterritorial reach that is similar to the GDPR: it applies to all business operators that handle the personal information of individuals in Japan, regardless of the size of the business. The APPI now also distinguishes between personal information and "special care-required" personal information – what might be referred to as "sensitive information" under certain data protection laws (for example Canada) – and imposes stricter requirements on the processing of this information, which includes medical history, marital status, race and religious beliefs. In contrast to other data protection laws, the APPI provides individuals with a private right of action whereby they can sue a business that collects their personal information if the business fails to respond to an APPI-based request, such as an access or rectification request, within two weeks.

(ii) China

China currently has two primary legislative documents and a significant guidance document serving as the base of its data protection regime: the Decision of the Standing Committee of the National People's Congress on Strengthening Network Information Protection adopted by the Standing Committee of the National People's Congress on 28 December 2012 (the "**Decision**"); the Cybersecurity Law,[17] which was adopted by the National People's Congress and came into effect on June 1, 2017; and the *Guide for Personal Information Protection within Information Systems for Public and Commercial Services* published by the National Committee of Information Security Standardization Technology on 15 November 2012 (the "**Guideline**"). In addition, China has over 100 laws, rules and regulations related to data protection that are overseen by various bodies across many sectors, resulting in a somewhat scattered data protection landscape. In light of this, the National People's Congress announced in 2019 its intention to introduce a comprehensive data protection law.[18]

- **The Decision** provides a set of principles and obligations related to data protection, although it does not set out any consequences or penalties for non-compliance.

- **The Cybersecurity Law** imposes data protection obligations on businesses that are "network operators", essentially businesses that have some online operations, including an email network. Such obligations include implementing adequate safeguards, mandatory breach notification and increased accountability for data handling within businesses. The Cybersecurity Law also imposes domestic data localization requirements for sensitive personal information and prohibits businesses from collecting and selling individuals' personal information. Although the Cybersecurity Law indicates that consent is required to collect and use personal information, it

[16] Kojin jōhō no hogo ni kansuru hōritsu [Act on the Protection of Personal Information], Act No. 57 of 2003 (May 30, 2003).

[17] Zhonghua Renmin Gongheguo Wanglao Anquan Fa [Cybersecurity Law] (promulgated by the Standing Comm. Nat'l People's Cong., Nov. 7, 2016, effective June 1, 2017).

[18] Cao Yin, "Lawmakers, political advisers focus on personal data protection", *China Daily*, (20 March 2019).

does not contain any provisions about whether consent should be opt-in or opt-out, and neither do any of the other data protection rules.

- **The Guideline** is nonbinding, but provides useful guidance for interpreting and applying terms and concepts that are included in the Decision and the Cybersecurity Law. For instance, the Guideline indicates that sensitive data is subject to increased protection, and that the determination of what is considered "sensitive" is contextual based on the industry in question and the "desires" of the individual.

II- ISSUES TO CONSIDER FOR ACHIEVING GLOBAL COMPLIANCE

This section lists a few considerations when assessing which data protection/privacy laws may find application and issues or challenges to consider.

a. Are you collecting, using or sharing "personal information"?

(i) Determine the type of personal information that you manage, which may include:

- **Consumer information** such as payment information, purchase history and contact information, although some contact information may be excluded from the application of certain data protection laws.
- **Employee information**, such as qualifications (i.e. education, certifications), title, payroll information (i.e. salary, bank details), benefits information, etc. "Work product" information produced in the context of the employment, and contact information that is used to contact an employee in the context of their employment may excluded from the application of certain data protection laws.
- **Technical information** collected through the use of cookies and other trackers (i.e. browsing history, technical preferences, login credentials, geolocation) may be considered personal information in certain jurisdictions.
- **Biometric information** is subject to the application of data protection laws and may also be subject to additional laws that specifically govern this type of information. For example, in Quebec, the *Act to establish a legal framework for information technology* imposes additional obligations on organizations that collect and use this type of information,[19] as do laws in the states of Illinois,[20] Texas[21] and Washington.[22]

[19] CQLR c C-1.1.

[20] 740 ILCS 14/5.

[21] TEX. BUS & COM. § 503.001.

[22] WASH. REV. CODE § 19.35.

(ii) Determine the **sensitivity** of this information, which may be done using:

- **Enumerated list:** In some jurisdictions, the legislature includes a list directly in the law of information that is considered sensitive directly in the law. For example, the GDPR provides that the following are subject to additional protections: information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership; genetic information, biometric information, health information and information concerning a person's sex life or sexual orientation.

- **Contextual approach:** Under PIPEDA (Canada) and the data protection laws in China, for instance, sensitivity is determined based on the context in which the information is used and collected, taking into account the reasonable expectations of the individual. Under this approach, certain types of information are considered inherently sensitive while others can be considered sensitive based on the unique circumstances of a situation or individual.

(iii) Determine is this information is still subject to data protection laws:

- **Anonymized information** is information that can no longer be linked to an identifiable individual. This may be information that has been separated from its direct identifiers as well as some of its indirect identifiers. While truly anonymized information may not be subject to data protection laws, this threshold may be quite high. For example, under Canadian law, information will 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*. Therefore, it is generally considered that achieving true anonymization is extremely difficult and it is more likely that information referred to as "anonymized" is actually pseudonymized rather than truly de-identified.

- **Pseudonymized information** is information that has been separated from its direct identifiers so that linkage to an identifiable individual is not possible without additional information that is held separately to ensure non-attribution. Due to the possibility of re-identification, it is therefore generally considered that pseudonymized information remains subject to data protection laws (for examples under the GDPR).

- **Publicly available information** or information from public sources may be excluded from certain data protection laws, but note that some jurisdictions (for example Canada) still regulate the acceptable uses of this type of information.

b. Are you responsible for this information?

Determine if you are a "data controller" or a "data processor":

The data controller is the organization that alone or jointly with others collects, uses and discloses personal information for its own purposes and is generally "in control" of how the information is retained and what it is used for. The data controller is generally the organization that is in direct contact with the individual, i.e. through its website or storefront. The data controller remains responsible for the

protection of the information under its control, and is therefore responsible for ensuring that data processors provide adequate protection for the information.

The data processor is the organization that processes personal information on behalf of the data controller, and does not use the personal information for its own purposes. For example, in certain jurisdictions, such as under the GDPR, there are different responsibilities and liabilities for data controllers and data processors.[23] In Canada, the distinction is less severe, although many of the responsibilities and relationships between organizations remain the same. For instance, under PIPEDA, the organization that collects the information from the individual for its own purposes remains responsible for that information and in certain situations, such as when a service provider is located outside Canada, must ensure that the service provider provides adequate protection for the information.

c. Where is the business operating?

Some data protection laws apply based on where an organization is located, while others apply based on where the individual is located or where they reside. For instance, the GDPR, has an explicitly extraterritorial reach and applies to organizations that collect and use the personal information of EU residents if the organization intentionally targets its goods or services to them, regardless of where the organization is located.

On the other hand, certain laws such as PIPEDA (Canada) apply to organizations that are collecting, using or disclosing personal information "in the course of commercial activities," but is silent with respect to territoriality. "Commercial activity" tends to be given a broad interpretation and includes any transaction, acts or conduct or any regular course of conduct that is of a commercial character. Therefore, to determine whether PIPEDA applies to an organization, the federal privacy regulator in Canada will consider whether there is a "real and substantial link"[24] between its commercial activities and Canada. Like under the GDPR, this determination takes into consideration whether an organization *targets its goods or services at Canadians*, and whether it collects the personal information of Canadians, but it also considers other connecting factors such as whether the organization rents space in Canada to operate a commercial activity or employs Canadians.

That being said, privacy regulators in Canada tend to take the position that they have jurisdiction when they receive a complaint about an organization, and therefore some organizations err on the side of caution and comply with data protection laws that may not explicitly apply to them.

d. Using personal information and consent

Organizations must generally obtain consent from an individual to collect, use and disclose their personal information under most data protection laws. Whether the consent required is express (opt-in) or implied (opt-out) may vary depending on factors such as the sensitivity of the personal information and the reasonable expectations of the individual. Furthermore, some data protection laws, such as PIPEDA (Canada), require that the purpose for which the personal information is being collected, used and

[23] For instance, a data processor must inform a data controller of any breach of security safeguards involving the information under the controller's control, and it is the data controller that must then inform the individual of the breach.
[24] *AT v. Globe24h.com*, 2017 FC 114 at para 50-51.

disclosed be reasonable, regardless of the consent obtained. Therefore, consent alone is not always sufficient.

- **Type of consent:** ***Implied consent*** may be acceptable in most situations, such as where non-sensitive personal information is being collected and used for a purpose that the individual would consider reasonable, whereas ***express consent*** may be required in situations where sensitive personal information is used for non-essential purposes, or purposes that an individual would not expect. For instance, sensitive information should not be used for targeted advertising purposes unless express consent has been obtained. As discussed above, the determination of what is sensitive information can be contextual under some laws, such as under PIPEDA (Canada), or can be based on an enumerated list, such as under the GDPR.

- **Meaningful consent:** In order to be considered valid, some data protection laws require that consent meet certain conditions. For instance:

    - Under the **GDPR**, a request for consent must be clearly distinguished from other matters and presented in an intelligible and easily accessible form, using clear and plain language. Consent must then be freely given and can only be a condition of a contract if it is necessary for the performance of that contract.

    - Under **PIPEDA** (Canada), consent is considered "meaningful" if individuals are adequately informed of important details about what their information will be used for, to whom it will be disclosed, and what the possible risks of harm are associated with the collection, use or disclosure of their personal information. Organizations generally inform individuals of these details via privacy notices, which must be written in clear, easy-to-understand language and clearly indicate if an individual has a right to withdraw their consent and how they can do so.

e. Sharing personal information

Consent is generally not required for an organization to **transfer information for processing** to a third party organization, such as to a service provider. That being said, under most data protection laws, the transferring organization or "data controller" remains responsible for the protection of the transferred information and must therefore ensure that the service provider organization has adequate safeguards in place.

- **Sharing within the same corporate group:** Under some data protection laws, organizations in the same corporate group may be able to share information for processing among themselves without additional formalities and without incurring significant risk given the increased transparency and accountability between the entities. For instance, under the GDPR, organizations in the same corporate group can transfer information amongst themselves under Binding Corporate Rules (BCRs), which are internal codes of conduct. However, under other laws such as PIPEDA (Canada), organizations in the same corporate group are still considered third parties and the formalities listed below, such as entering into a formal written agreement, may be required in order to remain compliant.

- **Sharing with third party service providers/vendors:** Sharing information with external third parties acting as service providers – often requires at a minimum:

    - **A formal written arrangement**, updated periodically and in the case of material changes, which should generally include details about the following:

        - ✓ what personal information is being handled by the third party, including both information shared by the organization and any information collected directly by the third party on behalf of the organization;
        - ✓ what specific rules, regulations and standards need to be complied with in the handling of the information;
        - ✓ the roles and responsibilities of key stakeholders within both organizations for the handling of the personal information, including responsibilities for specific functions, decision-making, safeguards and breach response;
        - ✓ information security obligations;
        - ✓ acceptable uses of the information;
        - ✓ retention and destruction obligations; and
        - ✓ reporting and oversight arrangements to ensure compliance with the above, including reporting obligations in the case of a breach that could compromise the personal information.

    - **A structured program for monitoring compliance against the obligations laid out in the arrangement**. The program should be suitable to the scope and sensitivity of the personal information being handled. It should include:

        - ✓ mechanisms for periodic reporting by the third party on the handling of the personal information; and,
        - ✓ where scope and sensitivity of the personal information handled is significant, mechanisms to ensure periodic external assessment (by the organization or an appropriate third party) of compliance with the full range of obligations described in the written arrangement.

- **Cross-border transfers:** When information is transferred across borders, some data protection laws impose additional obligations:

    - Under the **GDPR**, there is a distinction between third countries that are "secure" and "unsecure". Secure countries have received an adequacy decision from the European Commission confirming that they provide sufficient data protection, whereas unsecure countries have not. Therefore, if an organization in the EU is transferring personal information for processing to an organization in an unsecure country, it must use another means to ensure adequate protection for the information, such as standard contractual clauses or certification of the data processing procedure, or obtain the express consent of the individual. Organizations can also transfer information across borders to other entities in the same corporate group under Binding Corporate Rules, discussed at the beginning of this section.

- Under **PIPEDA** (Canada), organizations must be transparent by providing notice to individuals that their information will be transferred to a third party in another country for processing, and that while there, their information could be accessed by the courts, law enforcement and national security authorities of that country. Organizations must also use contractual or other means to ensure that the third party will provide a comparable level of protection for the information as it would receive from the organization itself in Canada.

f. Risks of non compliance

Risks of non-compliance may with data protection laws may include reputational damages, loss of market value, derivative shareholder's lawsuits, and well as the risks detailed in this section.

(i) Canada

The Office of the Privacy Commissioner of Canada ("**OPC**") can investigate **complaints** made regarding the personal information handling practices of an organization, and issue a report of findings following its investigations. If an organization does not comply with PIPEDA after the OPC publishes its findings, the OPC can apply to the Federal Court to commence a *de novo* hearing on the issues outlined in its report. The Federal Court can then order the organization to correct its practices in order to comply and award damages to the complainant, including for any humiliation suffered.

- An organization that fails to comply with the mandatory breach notification requirements under PIPEDA can also be liable to **regulatory fines** of up to $100,000.

- Violation of **common law/civil law privacy rights** can also result in civil lawsuits (including class actions) and liabilities for compensatory damages and, in appropriate circumstances, punitive damages. Privacy class actions are also a threat in terms of monetary damages for privacy violations. The Court of Appeal for Ontario in the decision Jones v. Tsige recognized for the first time in Canada a new tort of "intrusion upon seclusion" in 2012. This new tort has made privacy class actions potentially viable, because it appears to permit privacy breach claims to be advanced for compensation without proof of harm (i.e. economic harm) and without regard to the victim's individual circumstances.

(ii) Europe

The GDPR requires each EU Member State to designate an independent, public authority to oversee compliance with and enforce the GDPR. These authorities, generally known as "supervisory authorities" or "data protection authorities" ("**DPA**"). DPAs have many enforcement and oversight responsibilities, including investigating complaints and performing audits of data protection measures, as well as documenting infringements of the law and any corrective actions taken.

When a DPA determines that an organization is not in compliance with the GDPR, it can take a **range of actions**, such as issuing warnings or reprimands, imposing temporary or permanent bans on data processing, ordering the rectification, restriction or erasure of data, or suspending data transfers to third countries.

The DPA can also issue **administrative fines**, which vary in value depending on the article infringed: fines for infringements of articles relating to conditions for children's consent, processing that doesn't require identification, general obligations of processors and controllers, certification and certification bodies can amount to €10 million or 2% of annual global turnover – whichever is higher; fines for infringements of articles relating to data processing principles, lawfulness of processing, conditions for consent, processing of special categories of data, and data transfers to third countries or international organisations can amount to €20 million or 4% of annual global turnover – whichever is highest.

(iii) United States

The Federal Trade Commission ("**FTC**") enforces federal consumer protection laws as well as sector specific laws that contain privacy protections such as the *Fair Credit Reporting Act*, the *Children's Online Privacy Protection Act* and the *Telemarketing and Consumer Fraud and Abuse Prevention Act*. It also enforces the *Federal Trade Commission Act,* which prohibits organizations from engaging in unfair methods of competition and unfair acts or practices that affect commerce. It is on the basis of this Act that the FTC has primarily ordered organizations to adequately protect the privacy of consumers and has issued **significant fines** and reached significant settlements with organizations that fail to do so. For instance, in 2019, the FTC reached a $5 billion settlement with Facebook after it investigated the Cambridge Analytica Scandal and other privacy breaches.

III- PRIVACY GOVERNANCE AND BENCHMARKING

IAPP (the International Association of Privacy Professionals) and EY published their fifth annual *Privacy Governance Report* ("**Report**") on September 24, 2019.[25] The authors of the report surveyed companies across the globe to determine privacy governance trends. The Report aims to understand the structure of businesses' privacy programs (e.g., budget, staffing, career development), measure privacy compliance efforts (this year, with a focus on compliance with the GDPR and the CCPA) and identify recent trends in the daily routines of privacy and data protection professionals.

Since the survey respondents are from all around the world, the responses and trends are relevant for businesses that have global operations and which are in the process of benchmarking or updating their privacy governance framework. The following privacy governance topics of the Report are more specifically relevant: the role of the board of directors in privacy governance, the types of issues reported to the board, the privacy role and responsibilities within businesses, the management of third-party vendors, and the types of data subject requests that organizations receive.

a. Respondents

The survey respondents are privacy professionals in various roles (*e.g.* data protection officers mandated by the GDPR, privacy officers, chief privacy officers, privacy analysts, *etc.*), from various jurisdictions, industries and business sizes.

[25] "IAPP-EY Annual Governance Report 2019" (September 2019) available online at https://iapp.org/resources/article/iapp-ey-annual-governance-report-2019/.

- **Jurisdiction:**, 39% of the respondents are from the U.S., with the remaining from Canada (6%), the EU (33%), the UK (13%), and other countries (7%).
- **Industries:** These respondents are from various industries including tech (22%), (financial services (22%), healthcare and pharmaceuticals (9%), government (5%), consulting services (3%) and other (39%).
- **Size:** Most respondents come from medium or large companies with 1-4.9K employees (21%), 5-24.9K employees (24%), 25k-74.9K employees (11%), and over 75K employees (12%).

Interestingly, the Privacy Governance Report mentions that more often than in past years, survey respondents are lawyers, general counsel in particular, which may be signaling either promotion of privacy professionals to the GC role or (more likely) adoption of privacy responsibilities by GCs who previously did not pay as much attention to this issue.

b. Role of the Board

In the last few years, boards of directors have started to recognize privacy issues as significant legal and reputational risks. The Privacy Governance Report raises that while the role of the board of directors has always been important to privacy governance, the FTC further elevated the board's privacy role in its recent settlement order with Facebook over the Cambridge Analytica matter. In that case, the FTC not only levied a $5 billion fine on Facebook, but also required the company's board to create a special independent privacy committee to oversee and take responsibility for the company's privacy program. The SEC also reprimanded Facebook for not disclosing the risk that its customers might suffer privacy harms to its investors and ordered payment of $100 million as a fine. The Report states:

> "Although such numbers are not as significant to a company with annual revenue exceeding $50 billion, as they might otherwise be they are eye-catching nonetheless and should result in greater attention to privacy issues at the highest corporate levels."

c. Reporting to the Board

It is interesting for businesses with global operations to consider to whom privacy leaders report within organizations. According to the Report, privacy leaders are most likely to report to the board if they are data protections officers (67%), if the company has less than $100 million revenue (39%), if the headquarters is located in the EU (35%), or if the company has less than 5,000 employees (29%).

The Privacy Governance Report states that in the U.S., the privacy leader reports to the board of directors in 10% of the situations, while this number is at 35% for the EU. When not reporting to the Board of directors, they report to the general counsel (35% of the time for the U.S. or 18% for the EU), or they report to the CEO (16% of the time for the U.S. or 25% for the EU).

We learn that when privacy topics are reported to the board, it is usually related to data breaches (68% of the time) or GDPR compliance (64% of the time). The other specific privacy topics reported to the board relate to privacy program key performance indicators (58%), progress on privacy initiatives (47%), privacy

litigation (38%), number of privacy complaints (36%), specific incidents (36%), privacy compliance developments (26%), plans and strategies to prepare for the *California Consumer Privacy Act* ("**CCPA**") (23%), privacy budget details (22%), information regarding certifications and attestations (21%), material impact of CCPA (17%), or questions of data ethics (15%).

d. Privacy Role and Responsibilities

The location of the privacy role varies depending on the organizations. The Privacy Governance Report states that half of the privacy teams are located in the legal department, while 22% are located in regulatory compliance, 17% in privacy and data protection, 14% in information security, 10% in corporate ethics, 8% in information technology and 22% in another department.

On the issue of the type of responsibilities of the respondents by jurisdiction (comparing the U.S. vs the EU), the Report lists: GDPR compliance (72% U.S. vs. 97% EU), following privacy legislative developments (92% U.S. vs. 80% EU), service provider/vendor management (83% U.S. vs. 64% EU), ethical decision-making around data use (72% U.S vs. 56% EU), privacy-related subscriptions and publications (60% U.S. vs. 33% EU), preparation for the CCPA (80% U.S. vs.17% EU), redress and consumer outreach (47% U.S. vs. 33% EU), and privacy-related web certification and seals 38% (U.S.) vs. 21% (EU).

The Report shows that 33% of the respondents are very satisfied and 49% are satisfied with their jobs. Many also expect a promotion. Their main duties include dealing with privacy policies, procedures and governance; company awareness and training; addressing issues with products and services; following legislative developments; performing privacy impact assessments (PIAs); incident response; privacy-related communications; compliance with the GDPR; design and implementation of privacy controls; addressing privacy in product development; privacy-related investigations; and data inventory and mapping.

e. Managing Third Party Vendors

Canadian organizations generally remain accountable for personal information transferred to a third party vendor or service provider for processing, and must therefore use measures to ensure that this personal information remains adequately protected while in the hands of the third party. It is often difficult for organizations to determine what types of measures they should take in this respect.

On this issue of third-party service providers/vendor management, the Privacy Governance Report says that:

- 94% of respondents are "relying on assurances in the contract" as their method to ensure processors live up to their GDPR and other privacy and security obligations – with 88% confirming that the top consideration for processor selection is the existence of data protection and information security warranties;
- 57% of respondents require completion of questionnaires addressing data handling practices;
- 48% of respondents require third party attestations or certifications. ISO 27001 remains the favourite (44%). The other reported certifications are EU-U.S. Privacy Shield (23%), PCI (25%), SOC

2 Privacy (27%), ISO 27002 (16%), SOC 2 HIPAA (10%), ISO 27018 (9%), TrustArc (formerly TRUSTe) (3%) and CSA STAR (3%);

- 26% of respondents report conducting on-site service providers/vendor audits to vet their data-processing programs.

Other reported important considerations are carrying out due diligence of the service provider/vendor and limiting how much personal information such service provider/vendor receives.

f. Types of Data Subject Requests Received

Organizations often notice that when a highly publicized privacy incident or scandal occurs, there is an increase in data subject requests.

According to the Privacy Governance Report, most of the requests received from individuals in the previous year were access requests (68%), followed by right to erasure requests (60%), rectification requests (32%), processing restrictions and objections (31%) and data portability requests (14%).

The most difficult type of data subject requests received involve: locating unstructured personal information (56%), monitoring data protection/privacy practices of third parties (36%), ensuring data minimization (28%), developing an easy-to use, centralized opt-out tool (25%), anonymization (20%), making necessary changes to privacy notifications (9%), interconnected devices (9%), making changes to cookie policies (4%) and request involving artificial intelligence (4%).

***

Organizations wishing to determine best practices for their privacy governance program can use the Privacy Governance Report as a benchmarking tool when establishing their program. North American businesses may also use the Report as a preview of what to expect in terms of privacy governance if Canada or the U.S. adopts a more stringent privacy statute inspired by the EU GDPR.

Other topics addressed in the report include the salaries of privacy professionals within organizations and the budgets dedicated to privacy. On this topic, the Privacy Governance Report notes that businesses are increasing their privacy-related spending and that 55% of the respondents expect their privacy budget to rise in the next twelve months. This reflects the growing complexity of the global privacy landscape, with jurisdictions adopting privacy legislation at an increasing rate.

October 2019

For more information:

Éloïse Gratton
Partner and National Co-Leader, Privacy and Data Protection
EGratton@blg.com
416.367.6225 (Toronto) / 514.954.3106 (Montréal)

Elisa Henry
Partner and National Co-Leader, Privacy and Data Protection
EHenry@blg.com
514.954.3113