DATA PROTECTION AND CYBERSECURITY CONSIDERATIONS FOR CANADIAN ARBITRATION PROFESSIONALS

Kathleen Paisley [*]

International arbitration as practiced today is largely a digitalized process. Documents are exchanged virtually, whether through email or by way of digital platforms, and hearings and case management conferences are increasingly held remotely. This trend has been greatly amplified by the COVID-19 pandemic, which created a need to move swiftly to on-line platforms not only for the exchange of documents but for all aspects of the proceedings including merits hearings. The agility that was displayed by everyone from counsel to arbitrators to institutions is a testament to the flexibility of international arbitration as a dispute resolution mechanism.

The wide-spread use of technology has brought wide spread benefits to international arbitration in terms of time, cost, and other efficiencies, as well as reducing the impact on the environment. However, while technology certainly acts as a great facilitator of international arbitration, it also poses constraints on the process, including those related to data security and associated regulations. While these risks and regulations are not unique to arbitration, it is important that they be addressed and managed during international arbitration proceedings.

---

[*] Kathleen Paisley is an international arbitrator based in the US and Europe with significant experience in commercial and investor-State arbitration under all the major arbitration rules; she is triple qualified in law (Yale Law School), finance (MBA), and has passed the certified public accountancy exam (CPA); an expert in technology, life sciences, data protection and cybersecurity, she is co-chair of the ICCA-IBA Joint Task Force on Data Protection in International Arbitration, which authored the ICCA-IBA Roadmap to Data Protection In International Arbitration, and is a member of the ICCA-NYC Bar-CPR Working Group on Cybersecurity in Arbitration, which developed the Cybersecurity Protocol for International Arbitration.

For arbitration professionals based in Canada, the first consideration in terms of how data protection and cybersecurity requirements may apply to you is the Canadian *Personal Information Protection and Electronic Documents Act* ("*PIPEDA*"), which applies to organizations that collect, use, or disclose personal information in the course of commercial activities in Canada.[1] This encompasses arbitrations to the extent the activities being undertaken are considered commercial, which includes lawyers and likely arbitrators in their daily practice.[2]

Many of the *PIPEDA* requirements find their genesis in the European Union ("EU")[3] Data Protection Directive, which has now been replaced by the *General Data Protection Regulation* ("*GDPR*").[4] Since its entry into force in 2018, the application of the *GDPR* to international arbitration proceedings has been the

---

[1] *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5 [*PIPEDA*]. As discussed in footnote 9, this law is currently in the process of being amended, which may provide an opportunity for arbitration professionals to clarify the application of the Canadian data protection laws to international arbitration.

[2] *Ibid*, s 4 (1).

[3] This article refers throughout to the "EU", but the scope of application of the *General Data Protection Regulation* actually extends to the European Economic Area ("EEA"), which includes the 27 EU Member States plus Iceland, Liechtenstein, and Norway. Since the United Kingdom's withdrawal from the EU, the applicable data protection laws in the UK are the *Data Protection Act 2018* [UK *DPA 2018*), and the UK *General Data Protection Regulation* [UK *GDPR*].

[4] EC, *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 (General Data Protection Regulation) (Text with EEA relevance)*, *OJ L 119, 4.5.2016*, [2016] OJ, L 119 [*GDPR*]. OneTrust DataGuidance and Edwards, Kenny & Bray LLP have published an excellent comparison of the *PIPEDA* and the *GDPR*, see OneTrust DataGuidance & Edwards, Kenny & Bray LLP, "Comparing Privacy Laws: *GDPR* v. *PIPEDA*", online (pdf): *OneTrust DataGuidance* <www.dataguidance.com/sites/default/files/*GDPR*_v_*PIPEDA*.pdf>.

source of debate and some confusion. As non-compliance with the *GDPR* may trigger civil and/or criminal liability, including potential fines up to 4% of global gross revenue or 20 million Euros, whichever is higher. It is therefore important for arbitration professionals to consider the extent to which the *GDPR* applies to proceedings in which they are involved and, if so, what efforts should be taken to comply.

The *GDPR* is mandatory and there is no arbitration exception. However, while the *GDPR* applies to arbitration in principle, it says nothing about the means by which it should be applied to arbitration. The same is true of the *PIPEDA*, the UK DPA 2018, the UK *GDPR*, and most other data protection laws that may apply to international arbitration. Arbitration professionals subject to the data protection laws are therefore left to decide what data protection compliance requires in their cases, keeping in mind that even if one participant in an arbitration is subject to the *GDPR* or *PIPEDA,* this may impact the conduct of the arbitration as a whole.

Importantly, for those subject to the *PIPEDA*, compliance with the *PIPEDA* allows data to transfer freely to and from the EU, which is a significant competitive advantage for Canadian-based arbitration professionals when undertaking cases where the data processing is subject to the *GDPR*.

As explained in more detail below, the EU has recognized only fourteen countries, including Canada when the *PIPEDA* applies, as having data protection regimes that are equivalent to the *GDPR* such that personal data can transfer freely.[5] As a result, when a Canadian arbitration professional is involved in a case with EU-based participants, data can be exchanged with

[5] The European Union considers that the data protection laws of Andorra, Argentina, Canada (commercial organizations only), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland, United Kingdom, United States (Privacy Shield only) and Uruguay are adequate. At the time of writing, South Korea is in the process of adequacy discussions as part of its trade deal with the European Union.

him or her without concerns being raised about *GDPR* compliance. The same is not true for arbitrators based, for example, in the United States. This means that when EU-based parties are considering appointing arbitrators, those based in Canada would not pose data protection challenges during the arbitration in the way that arbitrators from countries that are not considered adequate may. However, this advantage comes at the price of *PIPEDA* compliance.

The importance of data protection to international arbitration led the International Council for Commercial Arbitration ("ICCA") and the International Bar Association Arbitration Committee to create a guide to these issues, which is now being finalized. The ICCA-IBA Roadmap to Data Protection in International Arbitration and its annexes seek to identify the data protection issues that may arise before, during, and after international arbitration proceedings, as well as the solutions that may be adopted to address them ("Draft ICCA-IBA Roadmap" or "Roadmap").[6] The Roadmap is not focused on a single data protection regime, but rather looks generally at the data protection rules applicable to arbitrations when a data protection regime built on the European principles (like *PIPEDA*) applies, regimes which are referred to here as "EU-based". The Roadmap includes examples and practice tips, and is accompanied by a set of annexes that provide greater detail, practical information, and checklists, as well as samples of data protection notices and a data protection protocol.

While the Roadmap will be the best guide to how data protection principles impact international arbitration proceedings, the purpose of this article is to synthesize that advice for Canadian arbitration professionals about when the data protection laws may apply to them and their cases and

[6] "The ICCA-IBA Roadmap to Data Protection In International Arbitration (Public Consultation Draft)", online (pdf): *International Council for Commercial Arbitration* <www.arbitration-icca.org/media/14/18191123957287/roadmap_28.02.20.pdf> ["Draft ICCA-IBA Roadmap"].

what this means in practice, taking *PIPEDA* into consideration. While the Roadmap is still in draft form and cannot be cited specifically for its content, reference is made generally to the Draft Roadmap where it would be applicable when finalized.

This article is set out in three Parts, as follows:

- Part 1 describes *PIPEDA*'s scope of application to arbitration professionals;
- Part 2 sets out the various ways in which data protection laws may apply to arbitration proceedings; and
- Part 3, the bulk of this article, explains the considerations that arbitration professionals should keep in mind in order to comply with data protection laws and how those rules may apply in the context of an arbitration proceeding with a focus on Canada.

This article draws examples from the *GDPR* because of its wide-ranging application and from the *PIPEDA* because of its importance to arbitration professionals based in Canada. For the convenience of readers, the *PIPEDA*'s list of "Fair Information Principles" and the text of the ICCA-NYC Bar-CPR Cybersecurity Protocol for International Arbitration are included as annexes.

An important word of caution before proceeding: this article is not intended to provide legal advice about compliance with *PIPEDA*, the *GDPR*, or any other specific law, but rather to give arbitration professionals a general understanding of the issues and how they may impact their practices and cases. If an arbitration professional has questions about the application of the data protection laws to them, they should seek legal advice.

I. WHEN DOES *PIPEDA* APPLY TO ARBITRATION PROFESSIONALS?

The nature of arbitration is such that significant amounts of personal data, sometimes including sensitive and criminal data,

is exchanged, often across borders. Such data exchanges and transfers are essential for the international arbitration process to function; however, they should be lawful under the applicable data protection laws and procedures put in place to ensure compliance with those laws throughout the proceedings.

The application of the *GDPR* to international arbitration has been the subject of significant discussion and publications, but the potential application of *PIPEDA* to international arbitration has thus far escaped scrutiny.[7]

PIPEDA is the Canadian federal data protection law. Adopted almost 20 years before the *GDPR*, it follows the principles established in the previous EU Data Protection Directive,[8] which was also the basis for the *GDPR*. Although *PIPEDA* does not apply to certain commercial activities undertaken solely within certain Canadian provinces, it applies to interprovincial or international transfers of personal information and hence is potentially applicable to international arbitration.

It is important to recognise that *PIPEDA* is currently under review and may be replaced with new legislation that is intended to better address the current digital reality. [9] These

---

[7] See e.g. "Draft ICCA-IBA Roadmap"; Clara-Ann Gordon, "The Impact of *GDPR* on International Arbitration—A Practical Guideline" (2019) 74:4 Disp Resol J 27; David Rosenthal, "Complying with the *General Data Protection Regulation* (*GDPR*) in International Arbitration—Practical Guidance" (2019) 37:4 ASA Bull 822; Kathleen Paisley, "It's All About the Data: The Impact of the EU General Data Protection Regulation on International Arbitration" (2018) 41:4 Fordham Intl L J 840.

[8] EC, *Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*, [1995] OJ, L 281/31 [*Data Protection Directive*].

[9] As a result of ongoing developments in technology, the Government of Canada introduced Bill C-11, or the *Digital Charter Implementation Act*, *2020* [*Act*], on November 17, 2020. If adopted, the *Act* would replace the privacy component of the *Personal Information Protection and Electronic Documents*

amendments may affect PIPEDA's application to arbitration, which is not addressed in this Article. Further, this amendment process provides a potential opportunity for the Canadian arbitration community to clarify the application of the Canadian data protection laws to international arbitrations.

The Canadian courts and the Office of the Privacy Commissioner of Canada ("OPC") have stated that *PIPEDA* has quasi-constitutional status.[10] At the same time, like the *GDPR*, *PIPEDA* seeks to balance the right of privacy of individuals with respect to their personal information and the need of organizations to collect, use, or disclose personal information in the course of carrying out their business.[11]

PIPEDA requires organizations to comply with a set of "Fair Information Principles" which are the foundation of Canadian personal information protection law. They require the following:

- Accountability
- Identifying purposes
- Consent

Act [*PIPEDA*] with the *Consumer Privacy Protection Act* [*CPPA*] and the *Personal Information and Data Protection Tribunal Act* [*PIPDT*].

[10] See *Joint investigation of Clearview AI, Inc by the Office of the Privacy Commissioner of Canada, the Commission d'accès à l'information du Québec, the Information and Privacy Commissioner for British Columbia, and the Information Privacy Commissioner of Alberta, PIPEDA Report of Findings #2021-001*, 2 February 2021, at para 61, citing e.g. *Nammo v Transunion of Canada Inc*, 2010 FC 1284 at paras 74—75; *Bertucci v Royal Bank of Canada*, 2016 FC 332 at para 34; *Alberta (Information and Privacy Commissioner) v United Food and Commercial Workers, Local 401*, 2013 SCC 62 at paras 19, 22; *Cash Converters Canada Inc v Oshawa (City)*, 2007 ONCA 502 at para 29, citing *Lavigne v Canada (Office of the Commissioner of Official Languages)*, 2002 SCC 53, and *Dagg v Canada (Minister of Finance)*, [1997] 2 SCR 403.

[11] *Englander v Telus Communications Inc,* 2004 FCA 387.

- Limiting collection
- Limiting Use, Disclosure, and Retention
- Accuracy
- Safeguards
- Openness
- Individual access
- Challenging compliance[12]

Organizations may collect, use or disclose personal information only for purposes that a reasonable person would consider appropriate in the circumstances, and only in line with the Fair Information Principles. [13] Annex 1 of this article provides a brief overview of these principles.

The OPC is responsible for overseeing compliance with *PIPEDA*. It has published a guide entitled "*PIPEDA* and Your Legal Practice – A Privacy Handbook for Lawyers",[14] which is now more than ten years old but remains a useful resource. The OPC Handbook provides an overview of how these principles could apply in the litigation context, which, although not arbitration-specific, provides useful guidance for arbitration professionals subject to *PIPEDA*.

The OPC takes the view that *PIPEDA* applies to legal professionals to the extent their work constitutes "commercial activity". As explained more fully below, this is likely to include lawyers' day-to-day operations and case work that is considered

[12] *PIPEDA*, Schedule 1.

[13] *PIPEDA*, s 5(3).

[14] *PIPEDA and Your Legal Practice - A Privacy Handbook for Lawyers*, online: *Office of the Privacy Commissioner of Canada* <www.priv.gc.ca/en/privacy-topics/business-privacy/gd_phl_201106/> [*Handbook for Lawyers*].

to be commercial. The extent to which this definition applies to investor-state cases is unclear, and is beyond the scope of this article.

PIPEDA applies to all to "organizations" that collect, use, or disclose personal information in the course of "commercial activities."[15] *PIPEDA* defines the term "organization" to include associations, partnerships, persons, and trade unions.[16] Further, the OPC has indicated that professionals engaged in commercial activities, including lawyers, are likely covered by *PIPEDA*. Hence, arbitration professionals would likely be considered to be "organizations" for purposes of the law and *PIPEDA* would be applicable to them to extent the particular activities being undertaken are considered commercial.

PIPEDA defines "commercial activity" as any "transaction, act, or conduct or any regular course of conduct that is of a commercial character."[17] Under this standard, law firms have been found to be engaged in commercial activities in their day-to-day operations when they perform services for their commercial clients.[18]

However, not all personal information that an organization, including an arbitration professional, collects, uses, and discloses is subject to *PIPEDA*. Rather, for *PIPEDA* to apply, it must be collected, used, or disclosed in the course of "commercial activity."

---

[15] *PIPEDA*, s 4(1).

[16] *PIPEDA*, s 2(1).

[17] *PIPEDA*, s 2(1).

[18] For example, under this standard, law firms have been found to be engaged in a commercial activity when they undertake credit checks on potential clients, and the obligations with respect to good record keeping and a client's right of access to their personal information have been found to apply to lawyers unless an exception applies.

This raises the question whether or which activities undertaken by arbitration professionals during arbitration proceeding are commercial activities. The OPC recently considered the application of *PIPEDA* to an insurance company's internal ombudsman office and its decision gives useful insight to the approach that may well be taken to *PIPEDA*'s application to commercial arbitration ("*Insurance Ombudsman Decision*"). Based on the reasoning of that decision, the OPC is likely to take the view that commercial arbitration is covered by *PIPEDA*.

Subsection 2(1) of *PIPEDA* defines "commercial activity" as "any particular transaction, act or conduct or any regular course of conduct that is of a commercial character, including the selling, bartering or leasing of donor, membership or other fundraising lists."

In deciding whether *PIPEDA* applied to the *Insurance Ombudsman Decision*, the OPC referred to the decision of the Federal Court of Canada in *State Farm*.[19] The court applied a narrow interpretation of "commercial activity" and found that personal information collected by an insurer for the purpose of defending a claim against its insured was not subject to *PIPEDA*, even though the information was collected before any claim had been commenced. The case involved an automobile accident between a complainant and a woman insured by State Farm who, in anticipation of potential litigation, hired private investigators to conduct surveillance on the complainant.

In deciding that *PIPEDA* did not apply, the court stated the following:

> The primary characterization of the activity or conduct in issue is the dominant factor in assessing the commercial character of that activity or conduct under [the Act], not the

[19] *State Farm Mutual Automobile Insurance Company v Privacy Commissioner of Canada*, 2010 FC 736 [*State Farm*].

> incidental relationship between the one who seeks to carry out the activity or conduct and third parties.[20]

Applying that test in its *Insurance Ombudsman Decision*, the OPC looked to the dominant purpose for the information being collected or generated in the course of the Ombudsman dispute resolution process. Since the data collection arose out of commercial activity between the complainant and the respondent, the OPC reasoned that *PIPEDA* would apply "on account of the commercial activity between the complainant and the Respondent, the ensuing relationship between the complainant and the Ombudsman falls under the scope of the Act." [21] Under the reasoning, commercial arbitration cases brought under arbitration agreements between commercial actors would be considered commercial activities covered by *PIPEDA*.

In deciding that the ombudsman proceeding was covered by *PIPEDA*, the OPC also considered the fact that *PIPEDA* contains an express exemption to the right of access for information gathered in the context of formal dispute resolution procedures. The OPC noted that "the very presence of … an exemption to provide an individual with access to personal information under the Act indicates that information relating to a formal dispute resolution process is capable of falling under the Act."[22]

The OPC's reasoning in the *Insurance Ombudsman Decision* is consistent with the approach taken in the Handbook for Lawyers, published five years earlier, which states "For example, the collection, use or disclosure of personal

---

[20] *Ibid* at para 106.

[21] *An insurance company's internal ombudsman office is not a "formal dispute resolution process" under PIPEDA*, *PIPEDA Report of Findings #2021-001* (Ottawa: Office of the Privacy Commissioner of Canada, 2021) [*Insurance Ombudsman Decision*].

[22] *Ibid.*

information in connection with litigation involving commercial organizations may well be carried out in the course of commercial activities, as distinguished from a personal injury claim involving individual litigants in their personal capacity."[23] For this reason, the collection, use, or disclosure of information carried out in connection with arbitrations of commercial disputes, and perhaps all arbitrations involving commercial parties, may be covered by *PIPEDA*.

Therefore, arbitration professionals based in Canada should consider whether *PIPEDA* may apply to them and the arbitrations in which they are involved, and what this requires in practice.

The remainder of this article is based on the premise that arbitration professionals will generally be considered to be covered by the *GDPR* or *PIPEDA*, such that the data protection rules apply to them during arbitration proceedings. This creates obligations, but also potential benefits because, if *PIPEDA* applies to one arbitration professional during an arbitration while other participants in the same arbitration are subject to the *GDPR*, this allows the free flow of information among them, effectively equating *PIPEDA* compliance with *GDPR* compliance for all practical purposes. As a result, it is easier to include Canadian arbitration professionals in cases where the *GDPR* applies.

[23] *Handbook for Lawyers*, *supra* note 14.

II. WHEN DO THE DATA PROTECTION LAWS APPLY DURING ARBITRATION PROCEEDINGS?

1. Coverage of Data Protection Laws

The GDPR and other EU-based data protection laws apply whenever: "personal data" [24] about a "data subject" [25] is "processed" [26] during activities falling within their jurisdictional scope. These concepts are broadly defined, and cover most information exchanged during an arbitration.

a. Personal Data of Data Subjects

Most of the information exchanged during a typical international arbitration contains personal data. Personal data is defined in the *GDPR* as "any information relating to an identified or identifiable natural person" or "data subject". [27]

---

[24] "Personal data" means any information relating to an identified or identifiable natural person (a "data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. See *GDPR*, art 4(1).

[25] "Data subject" means an identified or identifiable natural person. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person. See *GDPR*, art 4(1).

[26] "Processing" means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction. See *GDPR*, art 4(2).

[27] *GDPR*, art 4(1).

PIPEDA refers to information about an "identifiable individual."[28]

Under many laws, including the *GDPR*, it is irrelevant that the personal data is contained in a business-related document, such as work files, work emails, laboratory notebooks, agreements, construction logs, etc. Provided that the data relates to an individual who is identified or identifiable, it is considered to be personal data, and the individual to whom it relates is a data subject with rights.

Only the individuals who are identified or identifiable are referred to as "data subjects"; legal entities cannot be data subjects.[29] In the context of arbitration, the data subjects are the individuals mentioned in the evidence—the witnesses, the lawyers, etc.—which in a major arbitration can be hundreds of people, each of whom has rights under the data protection laws that cannot be waived by the parties. The *GDPR* applies stricter rules to sensitive personal data,[30] also referred to as "special category data," and largely prohibits the processing of criminal offence data without license.

b. Processing

EU-based data protection laws apply whenever personal data is "processed". Processing includes not only active steps

[28] *PIPEDA*, s 2(1).

[29] See *GDPR*, recital 14.

[30] The *GDPR* refers to "special category data", more commonly referred to as "sensitive data", which is defined as data which reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health, or data concerning a natural person's sex life or sexual orientation. The processing of special category data is allowed, among other reasons, where necessary for the establishment, exercise or defence of legal claims, or whenever courts are acting in their judicial capacity. See *GDPR*, arts 9(1), 9(2)(f).

such as collecting, using, disseminating, and deleting data, but also passive operations such as receiving, holding, organizing, and storing data. [31] Most activities undertaken in an international arbitration constitute processing.

2. Jurisdictional Scope of Data Protection Laws

The jurisdictional scope of EU-based data protection laws is broad, and they often apply extraterritorially. For example, the *GDPR* applies whenever personal data is processed:

- in the context of the activities of an establishment of a controller or a processor in the EU[32] or
- where the processing activities are related to the offering (targeting) of goods or services to individuals *in* the EU (regardless of their residence or citizenship).[33]

a. Data Processing in the Context of an EU Establishment

The *GDPR* applies to data processing by arbitration professionals when they have an EU establishment and the data processing takes place in the "context of the activities" of that establishment, wherever in the world the data processing occurs. The concept of "establishment" is defined broadly to include activities undertaken in the EU through "stable arrangements", regardless of the legal form those arrangements take.[34]

---

[31] See *Ibid*, art 4(2).

[32] *GDPR*, art 3(1).

[33] *Ibid*, art 3(2)(a).

[34] See "European Data Protection Board Guidelines 3/2018 on the Territorial Scope of the *GDPR* (Article 3), Version 2.1" (12 November 2019), online (pdf): *European Data Protection Board* <edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_3_2018_territorial_scope_after_public_consultation_en_1.pdf> ["Territorial Guidelines"]

Applying these criteria, arbitration professionals based outside the EU, including in Canada, should consider whether they undertake activities in the EU through stable arrangements and, if so, whether the data processing activities at issue are being carried out in the "context" of those activities. If the answer to both questions is affirmative, those data processing activities are likely to be covered by the *GDPR*.[35]

This determination will not always be straightforward. For example, when arbitrators based in Canada have of counsel or tenancy arrangements with firms or chambers within the EU, such arrangements would likely qualify as stable arrangements, and those arbitrators will then need to consider whether the data processing is being undertaken in the context of the activities of their chambers in the EU. In the case of London-based barristers' chambers, with the UK's departure from the EU the question would be whether the Data Protection Act 2018 and the UK *GDPR* applies; but for our purposes, the rules are generally the same (at least for now).

b. Data Processing Related to the Targeting Data Subjects Based in the EU

Even where the processing does not take place in the context of an EU establishment, the *GDPR* also applies "where processing activities are related to the offering of goods or services to such data subjects in the EU". This is also referred to as "targeting." This language appears to be geared at the

("[e]stablishment implies the effective and real exercise of activities through stable arrangements. The legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not the determining factor in that respect").

[35] *Ibid* ("determining whether processing is being carried out in the context of an establishment of the controller or processor in the Union for the purposes of Article 3(1) should be carried out on a case-by-case basis and based on an analysis in *concreto*" at 7).

targeting of individual consumers but could be applied more broadly.

When acting in a professional capacity, arbitration professionals typically do not target individual consumers, but rather other arbitration professionals and parties (typically companies). It is not clear whether these sorts of contacts trigger the application of the *GDPR*, but the fact that an individual is acting in a professional capacity does not prevent the application of the *GDPR* to him or her.[36]

Many EU-based data protection laws have similar jurisdictional requirements, but *PIPEDA* is silent on its extraterritorial application, although this is one of the issues under consideration for amendment.[37]

Under *PIPEDA*, the Federal Court of Canada has held that when a Canadians' personal information is collected, used, or disclosed from outside of the territory of Canada, *PIPEDA* will apply to the processing of personal information by an organization where there exists a "real and substantial connection" to Canada.[38] This standard applies to both domestic and foreign entities, and has been interpreted to the effect that

---

[36] *Supra* note 34. The "Territorial Guidelines" do not specifically address whether the *GDPR* applies to targeting outside of individual consumers, however, the guidelines contain numerous examples, all of which relate to the targeting of individual consumers, not in a professional context. This could imply that when data processing activities do not take place in the context of an EU establishment, the *GDPR* only applies when consumers are targeted, but it is not clear.

[37] For an excellent overview of the extraterritorial application of *PIPEDA*, see Wendy J Wagner, Christopher Oates & Sarah Boucaud, "Canada's Piece Of The Regulatory Pie: Application Of Canadian Data Privacy Laws To A Local Data Processor With A Global Reach" (14 January 2020), online: *Mondaq* <www.mondaq.com/canada/privacy-protection/883314/canada39s-piece-of-the-regulatory-pie-application-of-canadian-data-privacy-laws-to-a-local-data-processor-with-a-global-reach>.

[38] See *Lawson v Accusearch Inc (cob Abika.com)*, 2007 FC 125 at paras 38—43.

a foreign entity collecting personal information about an individual in Canada must comply with *PIPEDA*.

Also of potential importance to arbitration, the OPC recently issued a report in the AggregateIQ Data Services, Ltd. ("AIQ") investigation finding, which held that an organization based in Canada (which would include arbitration professionals as discussed above) is required to apply Canadian data protection laws to data that is collected abroad and transferred to Canada for processing.[39] The report finds that *PIPEDA* applies to data processors and service providers who use and disclose personal information, regardless of the jurisdiction in which that information was collected, stating as follows:

> Even where the information was collected in a different jurisdiction, whether that be the United Kingdom or the United States, AIQ is still required to meet its obligations under Canadian law with respect to its handling of that personal information in Canada. [9]

If this reasoning would be applied to international arbitration, , these cases stand for the proposition that: *PIPEDA* would apply to arbitrational professionals based outside Canada that process Canadians' personal information where there exists a "real and substantial connection" to Canada. Further, arbitration professionals based in Canada are subject to *PIPEDA* whenever they process personal data in Canada during an international arbitration, regardless of where the data was collected or whether it relates to a Canadian but this would not necessarily apply where Canadians process data abroad, for example, in the UK or Hong Kong.

---

[39] *Investigation Report P19-03/PIPEDA-035913: AggregateIQ Data Services, Ltd.*, 26 November 2019, online (pdf): *Office of the Information & Privacy Commissioner For British Columbia* <www.oipc.bc.ca/investigation-reports/2363> [*AIQ Investigation*].

III. WHAT DOES DATA PROTECTION COMPLIANCE REQUIRE FOR ARBITRATION PROFESSIONALS?

What does it mean when the data protection laws apply to you as an arbitration professional? This section will explain what data protection obligations may apply to arbitration professionals in the context of their practice, generally, and during the arbitral process. Again, it is not intended to be specific advice, but simply an overview.

If *PIPEDA*, the *GDPR*, the UK *Data Protection Act*, the UK *GDPR*, or another EU-based data protection law applies to you as an arbitration professional, it will be important for you to consider the impact this has on your practice and any cases in which you are involved. These laws usually will not apply to the case as a whole but rather to specific data processing activities depending on when, where, and by whom they are undertaken.

On a practical level this means that you will be required to comply with the data protection laws alongside the applicable arbitration law, rules, and any rules of evidence such as the IBA Rules on the Taking of Evidence, where they are applied. Furthermore, where the *GDPR* or *PIPEDA* applies, the doctrine of accountability requires those who process personal data subject to those laws to document the approach and measures they have taken towards compliance, which is important to demonstrate good faith efforts to comply should a dispute later arise.

1. What obligations may apply to arbitration professionals?

The data protection laws create a set of rules to protect the processing of personal data/information as well as stricter rules that apply to sensitive or special category data. The scope of these obligations depends on the applicable law and the arbitration professional's status under that law.

a. GDPR

Under the *GDPR*, the extent of the obligations depends on whether you are considered to be a data controller, a joint controller, or a data processor, each of which can be either a natural or legal person. Data controllers and joint controllers are primarily responsible for compliance and demonstrating compliance, whereas data processors, who process data on behalf of a controller, have more limited responsibility.

Controller: A data controller determines "the purposes and means of the processing of personal data" (see, e.g. *GDPR* Art. 4(7)). As discussed in the Draft Roadmap, applying this definition, during the course of an arbitration most participants are likely to be considered data controllers because the nature of their function is such that they control the purpose and means of the data they are processing in the context of an arbitration. Both barristers [40] and solicitors [41] are considered to be data controllers by relevant data protection authorities in the EU and the UK.

---

[40] Article 29 Data Protection Working Party, "Opinion 1/2010 on the Concepts of "Controller" and "Processor"" (16 February 2010) ("A barrister represents his/her client in court, and in relation to this mission, processes personal data related to the client's case. The legal ground for making use of the necessary information is the client's mandate. However, this mandate is not focused on processing data but on representation in court, for which activity such professions have traditionally their own legal basis. Such professions are therefore to be regarded as an independent 'controllers' when processing data in the course of legally representing their client" at 29) [emphasis added].

[41] The ICO is the UK Information Commissioner's Office, which applies the UK *DPA 2018* and the UK *GDPR*. The ICO has taken the view that solicitors are data controllers. *Ibid* at 29; ICO, "Data controllers and data processors: what the difference is and what the governance implications are, *Data Protection Act 1998*" (2014) at paras 40—43; Article 29 Data Protection Working Party, "Opinion 1/2010 on the Concepts of "Controller" and "Processor" ", (00264/10/EN WP 169, 2010).

Joint Controller: The *GDPR* has introduced the concept of joint controllers who jointly determine the purposes and means of the data processing.[42] Where the *GDPR* applies, each of the joint controllers is responsible for compliance with the *GDPR* and the joint controllers are jointly and severally liable for any data protection violation. They are required to make arrangements to allocate the risks involved, for example through a data protection protocol. However, the liability of a joint controller is limited to the processing for which that controller determines the purposes and means of the processing and does not extend to the overall chain of processing for which it does not determine the purposes and means, but this line can be difficult to draw in practice.[43]

In the context of an arbitration proceeding, distinguishing between (i) controllers, who are likely to be acting alongside other controllers with parallel responsibilities, or (ii) joint controllers acting jointly, may be difficult, and caution is warranted in light of recent decisions of the European Court of Justice ("CJEU") under the Data Protection Directive indicating that the notion of joint controllership is broadly interpreted. This emphasizes the importance of data protection compliance by all those involved in international arbitration proceedings.

Data processors: Data processors have more limited responsibilities under the *GDPR*. However, they must act under the instruction of a data controller in undertaking their tasks and cannot be responsible for deciding the purposes and means of the data processing and furthermore must be retained under a *GDPR*-compliant data processing agreement allowing the data controller to direct the processing and stop it at any time. This

---

[42] GDPR Art. 26(1).

[43] See "Judgment of 29 July 2019", *Fashion ID GmbH & Co KG v Verbraucherzentrale NRW eV*, C-40/17, ECLI:EU:C:2019:629 at paras 74, 85. See also "Judgment of 5 June 2018", *Wirtschaftsakademie Schleswig-Holstein*, C-210/16, EU:C:2018:388; "Judgment of 10 July 2018", *Jehovan todistajat*, C-25/17, EU:C:2018:551.

makes it unlikely that counsel, experts, arbitrators or institutions can be considered to be merely data processors during an arbitration because their function requires them to decide the purposes and means of the processing of personal data. However, depending on the context, tribunal secretaries, e-discovery professionals, transcribers, interpreters, and other vendors, may be considered data processors.

b. PIPEDA

PIPEDA does distinguish between data controllers, joint controllers, and data processors. Rather, as described above, *PIPEDA* applies equally to all organizations that collect, use or disclose personal information in the course of commercial activities.[44]

2. What does this mean in practice?

The *GDPR* applies generally to the processing of personal data, special category data, and, in the case of *PIPEDA*, in a commercial context. Special rules apply to certain types of special category data including highly sensitive data like medical records. However, there are no special rules for the processing of personal data depending on the context—the rules are generic and it is up to each person to apply them.

Arbitration is no different. The data protection laws apply to the processing of personal data by arbitration professionals in their general practice, in preparing for cases, and during the arbitral process. But there are no specific regulations applying to arbitration. This means that in any given arbitration there will be multiple data controllers, organizations, and others bound by different data protection laws in relation to the same personal data, each of whom has individual responsibility, liability, and potentially joint liability to ensure the protection of that personal data.

---

[44] *PIPEDA*, s 4 (1).

In considering what is required, generally speaking, the data protection laws require the issuance of data privacy notices, adopting appropriate data security measures and data breach procedures, ensuring that personal data processing and transfers are permissible under the law, minimizing personal data processing, putting in place data retention policies, and establishing procedures for addressing data subject complaints.[45]

a. Data Privacy Notices

Arbitration professionals subject to EU-based data protection laws are typically required to notify the data subjects about whom they process personal data of their data processing activities, which are referred to as "policies" under *PIPEDA*, rather than "notices." These notices or policies should be in plain language and the applicable statutes and regulations will describe what should be covered.[46]

All arbitration professionals should consider whether they are required to publish a general data privacy notice. Furthermore, in specific arbitrations with processing that is covered by the data protection laws like *PIPEDA* and the *GDPR*, the question arises as to how data subjects will be notified and by whom. In the case of a confidential arbitration, providing such notices could compromise the confidentiality of the arbitration.

It is also important to recall that data subjects include everyone who is identified or identifiable from the evidence and the pleadings, regardless of whether they have any relationship

[45] The Draft ICCA-IBA Roadmap provides a checklist of data protection issues that parties and their counsel may want to consider.

[46] See e.g. *GDPR*, arts 13—14. The Draft ICCA-IBA Roadmap provides in an annex examples of privacy notices for consideration by institutions, arbitrators, and legal counsel governed by the *GDPR*. This annex may be a starting point for arbitration professionals when deciding what to put in their privacy notices.

to the proceeding, and processing includes essentially everything that is done in arbitration cases. This means that, for many who lack a relationship with the data subject but will be processing their data, there may be no realistic means of providing notice.

In order to avoid overlapping notices, the *GDPR*, for example, provides exemptions from the notice requirements for data controllers who did not originally collect the data from the data subject, many of which will apply in arbitrations to those who did not directly collect data from individuals, like the arbitrators, an administering institution, and counsel. [47] However, even when those exemptions apply, it is important to determine whether someone has notified the data subject.

Therefore, arbitration professionals should consider whether they are subject to a notification requirement and, if so, to whom, as well as how the notification should be carried out without risking the integrity and confidentiality of the arbitration.

---

[47] Under the *GDPR*, when the data controller did not originally collect the personal data, as is often the case in international arbitrations, they are not required to provide notice where:

- The individual data subject already has the required information on the processing of his personal data;
- Providing information on the processing of personal data to the individual would be impossible;
- Providing such information to the individual would involve a disproportionate effort;
- Providing such information to the individual would render impossible or seriously impair the achievement of the objectives of the processing; or
- The data controller is subject to an obligation of professional secrecy regulated by EU or EU Member State law that covers the personal data.

See *GDPR*, art 14 (5), recital 62.

b. Data Security

When data protection laws such as *PIPEDA* and the *GDPR* apply to arbitrational professionals, appropriate data security measures are legally required.[48] However, those laws do not specify what security measures are required, but only that security measures must be "appropriate". Deciding what security measures are appropriate requires consideration of the potential risk to the individual data subjects, which is defined in *PIPEDA* by reference to the "sensitivity" of the data.[49]

Arbitration professionals subject to the data protection laws are required to apply appropriate security measures whenever they process personal data. Hence, these rules apply generally and in the context of specific cases.

The legal and arbitration community has published helpful guidance about cybersecurity, including the International Council for Commercial Arbitration (ICCA), the New York City Bar Association (NYC Bar) and the International Institute for Conflict Prevention (CPR): the ICCA-NYC Bar-CPR Protocol on Cybersecurity in International Arbitration.[50] The Protocol sets out 14 principles accompanied by explanatory commentary and examples, which provide guidance on establishing reasonable cybersecurity measures. These principles are set forth in Annex 2 of this article. Other guidance includes the International Bar Association Presidential Task Force's Guidelines on Cyber Security and the ICC's Note on Information Technology in

[48] See *GDPR*, art 32.

[49] *PIPEDA*, s 7.2(1)(a)

[50] "ICCA-NYC Bar-CPR Protocol on Cybersecurity in International Arbitration" (2020), online (pdf): *International Council for Commercial Arbitration* <cdn.arbitration-icca.org/s3fs-public/document/media_document/icca-nyc_bar-cpr_cybersecurity_protocol_for_international_arbitration_-_print_version.pdf>.

International Arbitration.[51] While these initiatives do not address security requirements in the context of data protection specifically, they are useful resources for applying the appropriateness test in relation to information security and determining how information security may be addressed in international arbitrations.

As described in the Protocol and the Roadmap, applying information security standards in an arbitration will depend on many factors, including the nature of the organizations involved, (including number of employees, their premises and data systems), the individual's role in the arbitration, their existing information security measures, the type of processing being undertaken and whether external service providers have been employed. The degree of security required also depends on the types of data being processed, including how valuable, sensitive, or confidential they are and the damage or distress that may be caused to the data subject if personal or sensitive data were to be compromised.

Note that for data protection purposes, these issues are related to the individual data subject, rather than the parties. In other words, the fact that the data may be commercially sensitive does not impact the extent of security required for data protection compliance, but may be very important for general security obligations. Increasingly in international arbitration practice, these issues are being addressed through the use of

---

[51] "International Bar Association's Presidential Task Force's Guidelines on Cyber Security" (October 2018), online (pdf): *International Bar Association* <www.ibanet.org/MediaHandler?id=2F9FA5D6-6E9D-413C-AF80-681BAFD300B0&.pdf&context=bWFzdGVyfGFzc2V0c3wxNTA4MzV8YXBwbGljYXRpb24vcGRmfGhlNC9oYWQvODc5NzA1MzM4Njc4Mi8yRjlGQTVENi02RTlELTQxM0MtQUY4MC02ODFCQUZEMzAwQjAucGRmfGNlZWMwNGQwZWM1ZjE1YmUxYTg1YjkzZDJjODVhMzUyN2YxNjg3ZjVlMzYwYzRjNWJkZjc3NzM4NmU2NzU2MTk>; "ICC's Note on Information Technology in International Arbitration", online (pdf): *International Chamber of Commerce* <iccwbo.org/content/uploads/sites/3/2017/03/icc-information-technology-in-international-arbitration-icc-arbitration-adr-commission.pdf>.

secure platforms for the exchange of written submissions and evidence.[52]

PIPEDA, for example, requires:[53]

- All the personal data an organization collects must be maintained securely, including being protected from personal loss, unauthorized access, and data theft;[54]
- The responsibility for protecting personal data lies with the organization (including arbitration professionals in possession of this data, which is required to designate someone to be accountable for *PIPEDA* compliance;[55]
- Personal data must be protected by physical measures, organization measures, and technological measures, irrespective of the format in which it is held;[56] and
- Data secrecy must be maintained as, in accordance with the sensitivity of the data, the more sensitive the data, the higher the required protection.[57]

---

[52] The Working Group on LegalTech Adoption in International Arbitration has also recently released a protocol for online case management in international arbitration, see "Protocol for Online Case Management in International Arbitration", online (pdf): *Latham & Watkins LLP* <www.lw.com/thoughtLeadership/protocol-online-case-management-international-arbitration>.

[53] For a helpful description of the applicable cybersecurity rules under *PIPEDA*, see Mitch Koczerginski, Lyndsay A Wasser & Carol Lyons, "Cybersecurity – The Legal Landscape in Canada", *McMillan Cybersecurity Bulletin* (October 2017), online: <mcmillan.ca/insights/publications/cybersecurity-the-legal-landscape-in-canada/>.

[54] *PIPEDA*, Schedule 1, art 4.7.1.

[55] *Ibid*, art 4.1.

[56] *Ibid*, art 4.7.3.

[57] *Ibid*, art 4.7.

Article 32 of the *GDPR* is more specific, requiring that, when deciding what information security measures are appropriate, consideration must be given to the "state of the art", implementation costs, data minimization, and the circumstances and risk level of the processing, with a focus on the risks to the data subject. The *GDPR* also provides that "appropriate" technical and organizational measures could include, as appropriate:

- The pseudonymization and encryption of personal data;
- The ability to ensure the ongoing confidentiality, integrity, availability, and resilience of processing systems and services;
- The ability to restore the availability of and access to personal data in a timely manner in the event of a physical or technical incident; and
- A process for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.[58]

Furthermore, under the *GDPR*, account must be taken of the risks that are presented by the processing, in particular from:

- Accidental or unlawful destruction;
- Loss;
- Alteration; or
- Unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed.[59]

[58] *GDPR*, art 32(1).

[59] *GDPR*, art 32(2).

In the specific context of arbitration proceedings, as set forth in the Roadmap and the Protocol, the data security obligations of all participants are inter-linked, and a breach of security by one will have an impact on all. This means that all those involved in an arbitration should:

- Consider what information security measures they already have in place;
- Employ information security measures appropriate to the size and use of their network and information systems;
- Take into account the state of technological development (although the cost of implementation can also be a factor);
- Employ information security measures appropriate to their business practices, the nature of the personal data processed, and the harm that might result from any data breach;
- Undertake a risk analysis in deciding what information security measures to employ and document the findings; and
- Provide notice to those affected if information security measures in place fail to prevent a data breach.

c. Data Breach Notices

Most EU-based data protection laws, including *PIPEDA* and the *GDPR*, require notifications of data breaches. In addition to these legal reporting requirements, counsel and arbitrators' general duties to protect the integrity of the proceedings or their express ethical obligations may require notification to the parties of a data breach, taking into consideration the risk that notification of a minor data breach may significantly disrupt the process. Given the risks associated with data breaches not only

to data subjects but also to the orderly conduct of the proceedings, questions concerning when notifications should be made should be addressed in advance of any breach.

Organizations subject to *PIPEDA* are required to:

- report to the Privacy Commissioner of Canada breaches of security safeguards involving personal information that pose a real risk of "significant harm" to individuals;
- notify affected individuals of any such breaches; and
- keep records of all breaches.[60]

Under *PIPEDA*, the definition of "significant harm" includes bodily harm, humiliation, damage to reputation or relationships, loss of employment, business, or professional opportunities, financial loss, identity theft, negative effect on credit rating, and damage to or loss of property.[61]

The *GDPR* has similar notification requirements, which obligate data controllers to notify the supervisory authorities in case of a data breach that is "likely to result in a risk for the rights and freedoms of the data subject" within 72 hours of their discovery of the breach. [62] The data subjects must also be notified of the breach if the data controller determines the risk to personal data be to be "high".[63]

This is a case-specific determination and, in the EU, for example, the burden to prove the absence of risk in a data

---

[60] Office of the Privacy Commissioner of Canada, "What you need to know about mandatory reporting of breaches of security safeguards", online: <www.priv.gc.ca/en/privacy-topics/business-privacy/safeguards-and-breaches/privacy-breaches/respond-to-a-privacy-breach-at-your-business/gd_pb_201810/>.

[61] *PIPEDA*, s 10.1(7).

[62] *GDPR*, arts 33—34.

[63] *Ibid*, art 34.

breach rests on the data controller.[64] Making this determination in the arbitration context requires consideration of the types of personal data being processed and the harm that could come to the individual data subjects (not the parties) from the incursion. It is therefore important to consider the nature of any personal, sensitive, and criminal offence data being processed and the harm that could befall the individual from its disclosure. It may be, for example, that notification is not required where the only personal data being processed for the arbitration is business email and other commercial correspondence and documentation, but this depends on the context and is highly specific. However, even where notification is not compulsory, a record of the breach must be kept.

If notification is required, *PIPEDA* and the *GDPR* both contain detailed provisions describing when the notification must be done, to whom, and what needs to be included. In the EU, for example, a data controller is considered to become aware of a breach when it has a "reasonable degree of certainty that a security incident has occurred that has led to personal data being compromised."[65] A breach notification must include the cause, the nature of the breach (if known), and recommendations as to mitigation efforts to reduce the risks of the breach.

d. Lawful Data Processing

In most jurisdictions, including in the EU and Canada, all processing of personal data covered by data protection laws must have a lawful basis. In other word, there must be a lawful reason for the processing.

---

[64] *GDPR*, arts 33—34.

[65] Article 29 Data Protection Working Party, "Guidelines on Personal data breach notification under Regulation 2016/679" (3 October 2017) at 11(last revised and adopted 6 February 2018).

There is no universal legal basis for lawful processing in the context of arbitration. Rather, the decision as to what data processing is lawful during an arbitration is fact-driven and case-specific. Depending on the circumstances of the case, the lawful bases may be different for different arbitral participants and for different types of personal data (e.g., witness data, data contained in the documentary evidence, sensitive data, criminal data). Lawfulness also requires that the personal data not be processed in a manner that is generally unlawful (for example in breach of confidentiality obligations).

The legal requirements for data processing can generally be met by obtaining the consent of a data subject. Under the *GDPR*, this needs to be informed consent in the case of general personal data processing, and explicit consent in the case of sensitive data, and it can always be withdrawn.[66] This makes it difficult to obtain valid consent in the arbitration context under the *GDPR*. If consent is withdrawn or refused, further processing must cease, which may complicate or even derail the arbitral process.[67]

Due to the inherent risk that consent may be refused or withdrawn, when the *GDPR* applies, it is generally preferable to rely on other legal bases. This is not to say that consent should never be employed, but rather that it should only be used as a basis for processing when all these considerations are acceptable under the circumstances. Indeed, the EU data

[66] *GDPR* ("'Consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her", art 4(11)).

[67] Article 29 Data Protection Working Party, "Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995" (25 November 2005) at 11.

protection authorities have referred to consent as a "false good solution".[68]

Under the *GDPR*, as set forth in the Roadmap, the following bases are generally best suited to data processing in the context of international arbitration:[69]

- **Personal data.** The processing of personal data is lawful when it is necessary for the purposes of the legitimate interests of the data controller or a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject requiring protection of their personal data. For example, in the arbitration context, the data subject's rights might override the legitimate interest in processing if the processing could raise significant risks to a data subject's profession or personal life and the personal data is not likely to be case-determinative.

- **Sensitive (special category) data.** The processing of sensitive (special category) data is lawful when it is "necessary for the establishment, exercise or defence of legal claims," which is called the "legal claims derogation".[70] The legal claims derogation will often be the preferred basis for processing sensitive data. In the arbitration context, it may apply to allow processing where, for example, the processing of sensitive data is likely to have a significant impact on a claimant or respondent's case. Personal data of children is also given

[68] EU Working Party, "Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995", WP 114, 25 November 2005, at 11.

[69] There are other bases for lawful processing under the *GDPR*, but the ones mentioned are the most likely to apply to arbitration.

[70] *GDPR*, art 9(2)(f).

special consideration, even where it would not otherwise be considered sensitive or special data.

- **Data Relating to Criminal Convictions and Offences or Related Security Measures.** In addition to requiring a lawful basis for the processing,[71] under Article 10 of the *GDPR*, the processing of personal data relating to criminal convictions and offences, or related security measures, must be carried out under the control of a supervising authority or, if the processing is authorized, by Union or Member State law. This makes it difficult to lawfully process criminal offence data. Arbitrators presiding over cases involving allegations of fraud or corruption or any other matter involving potential criminal activity should be particularly alive to this restriction and take measures to ensure the processing is lawful.

When relying upon legitimate interests as a basis for data processing, the *GDPR* requires a Legitimate Interests Assessment to be undertaken and recorded, which must be updated if events occur that might affect the original assessment. [72] A Legitimate Interests Assessment is a contemporaneous analysis undertaken to identify the particular interests being relied upon when a data controller invokes "legitimate interests" as the lawful basis for data processing, which may be important to show if issues are raised with a data protection authority.

This is probably the area where *PIPEDA* differs the most from *GDPR* personal data processing. *PIPEDA* is consent-based; consent is required for personal data processing in Canada unless an exception applies. In the words of the OPC, individual

[71] *GDPR*, art 6(1).

[72] *GDPR*, recital 47.

knowledge and consent is the "cornerstone" of *PIPEDA*.[73] Express or implied consent, or a prescribed exception to the consent requirement, must always be present in respect of any collection, use or disclosure of personal information including in the context of dispute resolution. Further, personal information may only be collected, used or disclosed for purposes that a reasonable person would consider appropriate in the circumstances.

The OPC recognizes the challenges of obtaining consent in the context of dispute resolution, and *PIPEDA* contains a number of relevant exceptions that may apply to the consent requirement in an arbitration. The Handbook states as follows with respect to litigation, which would also apply to arbitration:

> In many litigation matters, neither express nor implied consent will be applicable. This can be so where affected individuals are not parties to the litigation (*e.g.* where a corporate litigant's employee or customer personal information is involved). In such cases, lawyers and their clients must determine whether an exception to the knowledge and consent principle listed under section 7 of *PIPEDA* applies.[74]

The following are relevant *PIPEDA* sections that tend to arise in the arbitration context:

Collection:

---

[73] Policy and Research Group of the Office of the Privacy Commissioner of Canada, "Discussion paper exploring potential enhancements to consent under the *Personal Information Protection and Electronic Documents Act*" (May 2016), online: <www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2016/consent_201605/>.

[74] *Supra* note 14.

The collection of personal information without consent is permitted under paragraph 7(1)(b) where it is reasonable to expect that:

- the collection with the knowledge and consent of the individual would compromise the availability or accuracy of the information; and

- the collection is reasonable for purposes related to investigating a breach of an agreement or a contravention of the laws of Canada or a province, including the common law.

Use:

The use of personal information without consent is permitted under paragraph 7(2*)(d)* where the information was collected under paragraph 7(1*)(b)* above;

Disclosure:

The disclosure of personal information without consent is permitted by one of the exceptions listed under subsection 7(3), including the following:

- for the purpose of collecting a debt owed by the individual,

- where required to comply with a subpoena, warrant or order, or to comply with rules of court relating to the production of records, or

- when made to another organization and is reasonable for the purposes of investigating a breach of an agreement or a contravention of the laws of Canada or of a province that has been, is being or is about to be committed and it is reasonable to expect that disclosure with the

> knowledge or consent of the individual would compromise the investigation.[75]

It is for the Canadian arbitration professional to decide whether these exceptions apply to allow the processing of personal information without consent.

e. Lawful Data Transfer

EU-based data protection laws typically contain data transfer restrictions. Under the *GDPR*, whenever personal data is transferred outside the EU to entities or individuals who are not for other reasons already subject to the *GDPR*, transferors are required to make efforts to ensure that the personal data is protected after the transfer. As noted in the Roadmap, this leads to significant scope creep, even beyond the already broad territorial reach of the *GDPR*.

The *GDPR* rules respecting transfers of personal data to third countries apply to arbitration professionals bound by the *GDPR*. When an arbitration professional transfers personal data outside the EU to entities or individuals who are not subject to the *GDPR* or equivalent legislation or to international organizations, there must be a lawful basis for the transfer.[76]

It is worth noting that the *GDPR* treats data transfers to international organizations as transfers outside the EU, even if those organizations are located in the EU. This includes international organizations such as the Permanent Court of Arbitration, the World Bank, and the International Court of Justice, which are established under international law or by an agreement between countries. Accordingly, data transfers to

---

[75] *Handbook for Lawyers, supra* note 14.

[76] "Data transfer(s)" as used herein refers to third country data transfers of personal data outside of the EU or to an international organization, keeping in mind that immunities may apply to data transfers to international organizations. The EU adopts a broad concept of transfer and strict requirements for when it is lawful. See *GDPR*, arts 45, 46(1), 49.

these bodies must meet the *GDPR*'s requirements for international data transfers (but may be subject to privileges and immunities).[77]

The *GDPR* allows data transfers to third countries and international organizations where:

- the country has been deemed to provide adequate data protections, including *PIPEDA*;
- the data controller or data processor has put in place "appropriate safeguards" to protect the data through one of the means expressly prescribed by the *GDPR*;[78]
- one of a list of specified derogations apply, including where the processing is "necessary for the establishment, exercise or defence of legal claims";[79] or
- there are compelling legitimate interests pursued by the controller which are not overridden by the interests or rights of the data subject and the controller.[80]

Importantly, the EU has decided that "Canada is considered as providing an adequate level of protection for personal data transferred from the Community to recipients subject to the Personal Information Protection and Electronic Documents Act."[81] In other words, PIPEDA has been found to be equivalent

[77] *GDPR*, art 4(26) defining international organizations; *GDPR,* art 46(1) addressing transfers to international organizations.

[78] *GDPR*, art 46.

[79] *GDPR*, recital 52.

[80] *GDPR*, arts 45—49.

[81] EC, *2002/2/EC: Commission Decision of 20 December 2001 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided by the Canadian Personal Information Protection and Electronic Documents Act (notified under document number C(2001) 4539)*, [2002] OJ, L2 at 13—16 [*Canadian Adequacy Decision*].

to the GDPR, so data transfers may be freely made to Canadian arbitration professionals whenever PIPEDA applies.[82]

The same is not generally true of the United States, and indeed very few countries are considered by the EU to be adequate.[83] This provides a significant competitive advantage to Canadian-based arbitration professionals in cases where the GDPR is implicated, because it means that personal data can flow freely from the European Union to arbitration professionals based in Canada provided that they are subject to PIPEDA without having to follow the other requirements for data transfers described above. [84] These data transfer mechanisms will often require either entering into so-called standard contractual clauses developed by the EU, or limiting data transfers to what is necessary for the establishment, exercise or defence of legal claims, which is not necessary for Canadian arbitration professionals covered by PIPEDA.

Unlike the GDPR, PIPEDA does not provide a mechanism for establishing that a third-party organization has developed an adequate level of protection. Rather, under PIPEDA, transferring organizations remain responsible for personal information transferred to third parties, as the information is considered to remain under the control of the transferring organization.[85]

---

[82] *GDPR*, art 45(3). An adequacy decision is an EU decision made by reference to a set of criteria to the effect that a country's data protection laws are adequate. An adequacy decision allows data to be transferred without any further authorization or notice because adequate protections apply as a matter of law, as is the case with *PIPEDA*.

[83] *Supra* note 5.

[84] European Commission, "Questions & Answers on the Japan Adequacy Decision" (23 January 2019), online: *European Commission* <ec.europa.eu/commission/presscorner/detail/en/MEMO_19_422>. The EC has said the "decision on Canada applies only to private entities falling under the scope of the Canadian *Personal Information Protection and Electronic Documents Act*."

[85] *PIPEDA*, art 4.1.3.

Organizations must employ contractual privacy protection clauses or other means to ensure a comparable level of protection while the information is being processed by the third party. The OPC's Guidelines for Processing Personal Data Across Borders (the "Cross-border Guidelines") clarifies that appropriate means include, but are not limited to, ensuring that the third party:

- has appropriate policies and processes in place;
- has trained its staff to ensure information is properly safeguarded at all times; and
- has effective security measures in place.[86]

Further, *PIPEDA* does not distinguish between domestic and international transfers of information to third parties. It is not required to obtain additional consent for cross border transfers.[87] Although there is no requirement for additional consent for cross-border transfers under *PIPEDA*, the Cross-border Guidelines state that organizations must provide notice that:

- personal information may be sent to another jurisdiction for processing; and

[86] *Guidelines for Processing Personal Data Across Borders*, (January 2009), online: *Office of the Privacy Commissioner*, <www.priv.gc.ca/en/privacy-topics/airports-and-borders/gl_dab_090127> [Cross-border Guidelines].

[87] *Bank ensures openness and comparable protection for personal information transferred to third party, PIPEDA Report of Findings #2020-001,* (Ottawa: Office of the Privacy Commissioner, 2020), online: *Office of the Privacy Commissioner* <www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2020/*PIPEDA*-2020-001/>.

- while the information is in the other jurisdiction, it may be accessed by the courts, law enforcement, and national security authorities of that jurisdiction.[88]

f. Data Subject Rights

Data protection laws, including the *GDPR* and *PIPEDA*, grant data subjects important rights with respect to the processing of their personal data, several of which are likely to apply during the course of an arbitration. Data subject rights is an area where there are significant differences among countries with EU-based data protection regimes, and *PIPEDA* grants fewer express rights to individuals than the *GDPR* does to data subjects.

When the *GDPR* applies, data subjects are granted the following rights:

- the right of access and to obtain a copy[89] of the personal data being processed (referred to as a "data subject access request") except that "[t]he right to obtain a copy … shall not adversely affect the rights and freedoms of others"'[90]

- the right to request modification of their data, including the correction of errors and the updating of incomplete information;[91]

- the right to withdraw consent if consent was the basis for processing, which highlights why it is risky to rely on consent as a lawful basis;[92]

---

[88] See Cross-border Guidelines, *supra* note 86.

[89] *GDPR*, art 15(4).

[90] *GDPR*, art 7(3).

[91] *GDPR*, art 16; in contrast to the *GDPR*, no right of rectification exists under the *CPPA*, *supra* note 9.

[92] *GDPR*, art 15; *CPPA*, ss 1798.100(d), 1798.110, 1798.115.

- the right to object to processing where the lawful basis relied upon is a legitimate interest, in which case the controller must demonstrate that its compelling legitimate interest overrides the interests or the fundamental rights and freedoms of the data subject;[93] and

- the right to erasure—also referred to as the right to deletion or the right to be forgotten—which allows a data subject to request, under certain circumstances, that their personal data be erased.[94]

Arbitration professionals subject to the *GDPR* should also keep in mind that national laws may provide derogations from the *GDPR* with respect to data subject rights, which may impact the extent of the data subject rights in arbitration proceedings.

PIPEDA, on the other hand, does not contain an express list of data subject rights in the same manner as the *GDPR*, although this is something being considered for the revised legislation currently under consideration in Canada. However, some of the same rights apply under *PIPEDA*, including, for example, the right of access and the right to withdraw consent.

The right of access is the right most commonly enforced by data subjects. The *GDPR* provides that a data subject has the right to obtain from a data controller confirmation as to whether or not their personal data is being processed and, if it is, the right of access, which should include electronic access, to a broad range of information about that processing, as well as a copy of the data processed, provided that the provision of a copy does not interfere with the rights and freedoms of others. [95] However, the *GDPR* provides expressly that "the result of those

[93] *GDPR*, art 21; *CCPA*, s 1798.120.

[94] *GDPR*, arts 12, 17; *CCPA*, ss 1798.105, 1798.130(a), 1798.145 (g)(3).

[95] See *GDPR*, recital 63, art 15(4).

considerations should not be a refusal to provide all information to the data subject".[96]

During the arbitration process, arbitration professionals may receive requests from data subjects seeking to exercise their rights. These requests may come from any individual whose personal data is handled in the arbitration, including but not limited to individual parties, witnesses, experts, or even persons not directly involved in the proceedings but about whom personal data may have been adduced (*e.g.*, an employee of a party who is not personally involved in the proceedings but who was involved in the underlying transaction), and who believes that his or her data is being processed. Data subject requests must be addressed within a prescribed timeframe (30 days under the *GDPR*[97]) and it is therefore important to consider procedures for doing so in advance.

The right of access is difficult to apply during arbitration proceedings because providing a data subject with access to information about them being processed during an arbitration may violate the integrity of the proceedings or breach confidentiality. Arbitrators should be aware that invocations of the right of access may be made in a deliberate attempt to interfere with the proceedings.

The European data protection authorities have expressly taken the position that the right of access applies during dispute resolution proceedings. The *Working Document on Pre-trial Discovery for Cross Border Civil Litigation* states that data subject rights, including the right of access and to amend, may only be restricted:

> on a case by case basis for example where it is necessary to protect the rights and freedoms of others. The Working Party is clear that the rights

[96] *Ibid*.

[97] *GDPR*, recital 59.

> of the data subject continue to exist during the litigation process and there is no general waiver of the right to access or to amend.[98]

Under *PIPEDA*, individuals generally have a broad right to access their own personal information similar to the *GDPR*. However, unlike the *GDPR*, *PIPEDA* helpfully restricts an individual's right of access to personal data processed during a formal dispute resolution procedure, likely including commercial arbitrations. Specifically, an organization is generally not required to provide access to personal information if:

- the information is protected by solicitor-client privilege;
- the information would reveal confidential commercial information;
- providing access could reasonably be expected to threaten the life or security of another individual;
- the information was collected without the individual's knowledge and consent for reasonable purposes related to investigating a breach of an agreement or a contravention of the laws of Canada or a province; or
- the information was generated in the course of a formal dispute resolution process.[99]

As discussed above, the OPC decided in the *Insurance Ombudsman Decision* that the ombudsman procedure at issue in

---

[98] Article 29 Data Protection Working Party, "Working Document 1/2009 on pre-trial discovery for cross border civil litigation" (11 February 2009) at 12, online (pdf): <www.garanteprivacy.it/documents/10160/10704/ARTICOLO+29+-+WP+158+-+cross+border+civil+litigation.pdf/1595b252-efb3-460d-837d-c892b5d3e22a?version=1.2> ["Discovery Guidelines"].

[99] *Insurance Ombudsman Decision*, *supra* note 21.

that case was a dispute resolution procedure, but did not rise to the level of being "formal", so that it was *subject to* the right to access. However, the OPC's reasoning gives insight into why commercial arbitration agreed to between the parties and subject to binding arbitration rules would likely be considered a "formal dispute resolution" and therefore *not* subject to the right to access:

> A "formal dispute resolution process" suggests the presence of a framework, either legislated or agreed to by the parties to the dispute, as well as a process that takes place in accordance with recognized rules. This is consistent with an unpublished finding by our Office, which examined the Ombudsman's Office of a financial institution with a framework almost identical to that of the Ombudsman.[100]

Under the OPC's rationale in that decision, commercial arbitrations based on arbitration agreements entered into between commercial entities under recognized arbitration rules would seem to fall within this standard. As such, information generated in the course of commercial arbitration proceedings may not be subject to the right to access.

As noted by the OPC in that decision, it is important to keep in mind that in making this determination the OPC was "considering whether the process at issue should be exempted from the obligation to allow data subjects access to their data from the process" (thereby restricting their rights. The OPC noted in that regard that:

> Paragraph 9(3)(d) constitutes an exemption to an organization's obligation to provide an individual with access to personal information under the Act. Since the Act has been recognized as quasi-

[100] *Ibid.*

> constitutional legislation, the rights accorded under it should be given a liberal and purposive interpretation, and restrictions on those rights should be interpreted narrowly. In this case, any ambiguity concerning the scope of paragraph 9(3)(d) should be resolved in favour of granting access to personal information.[101]

This would caution in favour of reading the *Insurance Ombudsman Decision* narrowly.

When faced with a data subject access request during an arbitration proceeding, careful consideration should be given to whether an exemption applies (for example under PIPEDA), to the impact that meeting the request might have on others (both those involved in the arbitration and third parties), and to identifying and implementing measures to reduce any potential adverse impact on third parties or the proceedings themselves. For example, personal data relating to third parties may be redacted and access limited to those documents or portions thereof strictly necessary to meet the exact terms of the data subject's request, rather than adopting a blanket (and less onerous) approach. National courts have also suggested that striking a balance between different stakeholders' interests might involve obtaining undertakings to restrict the onward transfer of any information disclosed in response to the data subject access request.[102]

g. Data Minimization

Data minimization is a key component of data protection compliance, both as a requirement in itself and also as part of data security. Data minimization requires the collection and

[101] *Ibid*.

[102] *B v General Medical Council* [2018] EWCA Civ 1497.

retention of personal data to be limited to information that is directly relevant and necessary for a specified purpose.

Data minimization is required by *PIPEDA*:

> Principle 4 – Limiting Collection: The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. … Organizations shall not collect personal information indiscriminately. Both the amount and the type of information collected shall be limited to that which is necessary to fulfil the purposes identified.[103]

Data minimization is also a fundamental principle of the *GDPR*:

> Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.[104]

Data minimization is also part of good cyber security hygiene. Given the amount of personal data that is typically processed and transferred in the context of a dispute, data minimization is an important consideration.

As discussed in the Roadmap, data minimization is required in all stages of the arbitral process and requires those involved to ensure that the amount and type of personal data processed is adequate, relevant, and limited to what is necessary for the lawful purpose of the processing (i.e., preparing a case for arbitration, prosecuting, defending against, or deciding a claim, administering the proceedings, or retaining data in relation to the arbitration after completion of the proceedings). As discussed below, this is especially important during the

---

[103] *PIPEDA*, Annex 1.

[104] *GDPR*, art 5(1)(c).

document disclosure phase of the arbitration and supports limiting disclosure.

h. Data Retention

Similar to the rules requiring the minimization of personal data being processed generally, EU-based data protection laws contain express limitations on the retention of personal data.

The *GDPR* provides that:

> Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.[105]

PIPEDA imposes a similar requirement:

> Personal information shall be retained only as long as necessary for the fulfilment of [the purposes for which it was collected]. … Personal information that is no longer required to fulfil the identified purposes should be destroyed, erased, or made anonymous. Organizations shall develop guidelines and implement procedures to govern the destruction of personal information.[106]

These principles ensure that personal data is only stored for as long as necessary for the purpose for which it is being processed. As discussed in the Roadmap, in practice, this means that arbitration professionals, like all those covered by the data protection laws should:

- Retain personal data only for as long as reasonably necessary;

---

[105] *GDPR*, art 5(1)(e).

[106] *PIPEDA,* Annex 1.

- Be able to justify how long they retain personal data, which will depend on the purposes informed to the data subject for holding the data;

- Periodically review the data held, and erase or anonymize it when they no longer need it; and

- Carefully consider any challenges to their retention of data.

IV. WHAT DOES THIS MEAN FOR ARBITRATION PROCEEDINGS?

The nature of the arbitral process is such that significant amounts of personal data (sometimes including sensitive and criminal data) is exchanged and processed, often across borders. Such data exchanges, transfers, and processing are inherent to the international arbitration process. However, they must be lawful under the applicable data protection laws, and procedures must be put in place to ensure compliance with those laws throughout (and beyond) the proceedings.

At the outset of any dispute, long before any request for arbitration is filed, parties and their lawyers will review the facts by going back through the chain of events that led to the dispute. This will involve review of contemporaneous correspondence, usually starting from the contracting stage. Moreover, the possibility of document disclosure during an arbitration may require the parties and others to suspend their usual data destruction policies or to make changes to their usual retention or deletion processes to comply with a "litigation/arbitration hold" in contemplation of legal proceedings. All of these activities constitute the processing of the personal data subject to the data protection laws and must comply with those laws when they apply.

Data minimization is an important part of all EU-based data protection laws and should be practiced throughout the arbitration process. Data minimization obligations are particularly relevant in the selection, production, and disclosure

of documents.[107] The EU data protection authorities have suggested that data minimization is likely to require the following when making disclosures:

- Limiting the data disclosed to what is relevant to the dispute and non-duplicative;
- Identifying the personal data contained in the responsive material;
- Redacting or pseudonymizing unnecessary personal data;
- Considering confidentiality orders; and
- Ensuring proper data protection measures are in place after disclosure

Limiting disclosure to relevant documents is already standard practice in international arbitration, in order to reduce the volume of data disclosed. However, redaction of personal data is not common practice and may require significant additional time and effort. Technology, including artificial intelligence, may assist in both culling the data for relevance and in redacting personal data. However, these measures themselves constitute data processing, triggering data protection obligations, and can be costly and time-consuming.

---

[107] The European Data Protection Board has stated that "the principle of data minimization … emphasizes the need for personal data to be adequate, relevant and limited to what is necessary in relation to the purposes for which [it is] processed." See European Data Protection Board, "Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data Version 2.0" (2021) at 13, online (pdf): *Eurioean Data Protection Board* <edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf> [Data Transfer Guidance].

It is also important to keep in mind that data protection principles apply during the hearing and to the award. This means in the context of remote hearings, for example, the exchange of information and testimony during the hearing could be considered a data transfer subject to the restrictions imposed on such transfers. Further, any personal data included in the award must comply with the data protection rules, taking into account that the award may become public even in the context of confidential arbitrations (for example during enforcement proceedings).

As a procedural matter, it is important that in cases where an EU-based data protection law, like the *GDPR* or *PIPEDA*, applies to some or all those involved in the proceeding, data protection be considered at the initial procedural hearing or case management conference. This will allow the tribunal, together with the parties and their counsel, to consider the potential impact that data protection may have on the proceedings and to put measures in place to manage these issues and to avoid either party using them to its advantage. This may be complicated in the event that only one of the parties is subject to strict data protection obligations, which may lead to issues of inequality of treatment.

Issues to be considered include:

- Data security
- Potential impact of data protection on the exchange of information during the proceeding, including, for example:
    - Document disclosure
    - Hearing
    - Award
- Any necessary processes for:

- Addressing any data subject requests
- Data breach notification process
- Documenting compliance in a manner that can be shared with regulators if necessary

These issues are discussed in the Roadmap, which includes annexes addressing measures that may be employed during an arbitration. In cases where the impact of data protection is expected to be minimal, this may be limited to the inclusion of general language in the first procedural order or terms of reference that the parties will comply with such data protection measures and that they will ensure that such compliance will not impact the orderly conduct of the proceedings, including document disclosure, the hearing, the award, data subject access requests, data breach procedures, and the documentation of compliance. Language should also be included addressing data security and data breach procedures.

In cases where data protection may significantly impact the proceedings, a data protection protocol should be considered (and may be required) to ensure compliance among controllers and organizations with their parallel and interlinked obligations, as is the case in arbitration. For example, under the *GDPR*, a data protection protocol is required whenever joint controllers process personal data.[108]

As described in the Roadmap, a data protection protocol is an agreement on how data protection will be applied in a particular context. Data protection protocols can be usefully employed in arbitrations to manage the compliance obligations of all those responsible for data protection compliance throughout the arbitration.

---

[108] *GDPR art 26* ("Joint controllers shall in a transparent manner determine their respective responsibilities for compliance with the obligations under this Regulation.").

V. CONCLUDING THOUGHTS

International arbitration proceedings have become a digital process, which allows for significant benefits in terms of time, cost, and other efficiencies. However, while the wide-spread use of technology largely acts as a facilitator of international arbitration, it also introduces constraints on the process, including those stemming from data protection and related security requirements.

It is therefore important that data protection and security be addressed and managed during international arbitration proceedings. In this context, as described above, Canadian arbitration professionals should be aware that:

- The *GDPR* applies to arbitration professionals when they have an EU establishment and the data processing takes place in the "context of the activities" of that establishment wherever the data processing occurs in the world, and the same applies under the UK Data Protection Act and the UK *GDPR*.

- *PIPEDA* applies to arbitration professionals in the context of their commercial activities.

- *PIPEDA* and the *GDPR* may apply to international commercial arbitration proceedings.

- Where *PIPEDA* applies to an arbitration professional, personal data may freely transfer to them from the EU.

- *PIPEDA* is going to change, so it is important to keep apprised of developments.

- A good source of guidance on when and how data protection laws apply to international arbitrations is the Draft ICCA-IBA Roadmap to Data Protection in International Arbitration and its annexes, which will be finalized during 2021.

ANNEX 1

PIPEDA's FAIR INFORMATION PRINCIPLES

Where *PIPEDA* applies, it requires organizations engaged in commercial activities to comply with a set of legal obligations based on ten principles in relation to those commercial activities unless a relevant exception applies. These are:

Principle 1 - Accountability

An organization is responsible for personal information under its control. It must appoint someone to be accountable for its compliance with these fair information principles.

Principle 2 - Identifying Purposes

The purposes for which the personal information is being collected must be identified by the organization before or at the time of collection.

Principle 3 - Consent

The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.

Principle 4 - Limiting Collection

The collection of personal information must be limited to that which is needed for the purposes identified by the organization. Information must be collected by fair and lawful means.

Principle 5 - Limiting Use, Disclosure, and Retention

Unless the individual consents otherwise or it is required by law, personal information can only be used or disclosed for the purposes for which it was collected. Personal information must only be kept as long as required to serve those purposes.

Principle 6 - Accuracy

Personal information must be as accurate, complete, and up-to-date as possible in order to properly satisfy the purposes for which it is to be used.

Principle 7 - Safeguards

Personal information must be protected by appropriate security relative to the sensitivity of the information.

Principle 8 - Openness

An organization must make detailed information about its policies and practices relating to the management of personal information publicly and readily available.

Principle 9 - Individual Access

Upon request, an individual must be informed of the existence, use, and disclosure of their personal information and be given access to that information.[109]

An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

Principle 10 - Challenging Compliance

An individual shall be able to challenge an organization's compliance with the above principles. Their challenge should be

---

[109] This will not apply to arbitration proceedings when para 9(3)(a) of *PIPEDA* is engaged, which provides that an organization is not required to give access to personal information if the information is protected by solicitor-client privilege or, in civil law, by the professional secrecy of lawyers and notaries and para 9(3)(d) of *PIPEDA* states that an organization is not required to give access to personal information if the information was generated in the course of a formal dispute resolution process.

addressed to the person accountable for the organization's compliance with *PIPEDA*, usually their Chief Privacy Officer.[110]

Further, any collection, use or disclosure of personal information must only be for purposes that a reasonable person would consider appropriate in the circumstances.[111]

These principles are similar to those found in the *GDPR* and other EU-based data protection laws.

[110] Office of the Privacy Commissioner of Canada, "*PIPEDA* in Brief" (May 2019), online: *Office of the Privacy Commissioner of Canada* <www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-PIPEDA/PIPEDA_brief/>.

[111] *Ibid.*

ANNEX 2

ICCA-NYC BAR-CPR CYBERSECURITY PROTOCOL

FOR INTERNATIONAL ARBITRATION (2020)

(Without Commentary)

Scope and Applicability

Principle 1 The Cybersecurity Protocol provides a recommended framework to guide tribunals, parties, and administering institutions in their consideration of what information security measures are reasonable to apply to a particular arbitration matter.

Principle 2 As a threshold matter, each party, arbitrator, and administering institution should consider the baseline information security practices that are addressed in Schedule A and the impact of their own information security practices on the arbitration. Effective information security in a particular arbitration requires all custodians of arbitration-related information to adopt reasonable information security practices.

Principle 3 Parties, arbitrators, and administering institutions should ensure that all persons directly or indirectly involved in an arbitration on their behalf are aware of, and follow, any information security measures adopted in a proceeding, as well as the potential impact of any security incidents.

Principle 4 The Protocol does not supersede applicable law, arbitration rules, professional or ethical obligations, or other binding obligations.

The Standard

Principle 5 Subject to Principle 4, the information security measures adopted for the arbitration shall be those that are

reasonable in the circumstances of the case as considered in Principles 6-8.

Determining Reasonable Cybersecurity Measures

Principle 6 In determining which specific information security measures are reasonable for a particular arbitration, the parties and the tribunal should consider: (a) the risk profile of the arbitration, taking into account the factors set forth in Schedule B; (b) the existing information security practices, infrastructure, and capabilities of the parties, arbitrators, and any administering institution, and the extent to which those practices address the categories of information security measures referenced in Principle 7; (c) the burden, costs, and the relative resources of the parties, arbitrators, and any administering institution; (d) proportionality relative to the size, value, and risk profile of the dispute; and (e) the efficiency of the arbitral process.

Principle 7 In considering the specific information security measures to be applied in an arbitration, consideration should be given to the following categories:

(a) asset management;

(b) access controls;

(c) encryption;

(d) communications security;

(e) physical and environmental security;

(f) operations security; and

(g) information security incident management.

Principle 8 In some cases, it may be reasonable to tailor the information security measures applied to the arbitration to the risks present in different aspects of the arbitration, which may include:

(a) information exchanges and transmission of arbitration related information;

(b) storage of arbitration-related information;

(c) travel;

(d) hearings and conferences; and/or

(e) post-arbitration retention and destruction policies.

Process to Establish Reasonable Cybersecurity Measures

Principle 9 Taking into consideration the factors outlined in Principles 6-8 as appropriate, the parties should attempt in the first instance to agree on reasonable information security measures.

Principle 10 Information security should be raised as early as practicable in the arbitration, which ordinarily will not be later than the first case management conference.

Principle 11 Taking into consideration Principles 4-9 as appropriate, the arbitral tribunal has the authority to determine the information security measures applicable to the arbitration.

Principle 12 The arbitral tribunal may modify the measures previously established for the arbitration, at the request of any party or on the tribunal's own initiative, in light of the evolving circumstances of the case.

Principle 13 In the event of a breach of the information security measures adopted for an arbitration proceeding or the occurrence of an information security incident, the arbitral tribunal may, in its discretion:

(a) allocate related costs among the parties; and/or

(b) impose sanctions on the parties.

Principle 14 The Protocol does not establish any liability or any liability standard for any purpose, including, but not limited to, legal or regulatory purposes, liability in contract, professional malpractice, or negligence.