

**UNDER THE UNCITRAL ARBITRATION RULES (1976) AND NORTH
AMERICAN FREE TRADE AGREEMENT (NAFTA)**

Tennant Energy, LLC.

Investor

v.

Canada

Respondent

**QUESTIONS AND INVESTOR'S RESPONSE TO TRIBUNAL GDPR QUESTIONS
AND DATA PRIVACY QUESTIONS**

June 4, 2019

I. OVERVIEW

- 1) In its May 28, 2019 email to the parties, the Administrator, on behalf of the Tribunal, posed two questions to the Investor about the application of the General Data Protection Regulation 2016/679 (“GDPR”) to this arbitration.¹ This document provides the Investor’s response to those questions.
- 2) This arbitration is based upon claims brought under Chapter Eleven of the North American Free Trade Agreement (“NAFTA”). Those claims will be supported by thousands of pages of documentary evidence generated, controlled, and/or possessed by private parties and the government of the province of Ontario, Canada—including, but not limited to, documents from private sector proponents who sought contracts under Ontario’s green energy regulatory scheme. Among those private sector, proponents are a number of persons who would legally be considered to be European data subjects, as that term is defined by the GDPR.
- 3) As a result, there are several issues the Tribunal should consider, including:
 - making documents that contain personal data public without the consent of the data subjects;
 - how best to address confidentiality and handle data;
 - data production and redaction; and
 - the status of various arbitral participants and the actions each might need to take to address data privacy obligations.
- 4) The Investor hopes that this document will assist the Tribunal to address these issues.
- 5) Also, Appendix A sets out data privacy questions for the Tribunal, the Administrator, and Canada.

¹ Email from C. Tham to disputing parties - May 28, 2019 (C-12).

- 6) The GDPR applies if personal data is processed in connection with:
- the activities of an EU establishment;²
 - the offering of products and services to data subjects in the EU;³ or
 - monitoring the behaviour of data subjects in the EU.⁴
- 7) What is necessary to be considered an EU establishment is not precisely defined in the GDPR. However, GDPR Recital 22 states that an establishment “implies the effective and real exercise of activity through stable arrangements.” If an individual regularly resides in the EU and operates a business from there, he has an EU establishment.

1. SIR DANIEL BETHLEHEM, Q.C.

- 8) A resident of London, Arbitrator Sir Daniel Bethlehem has an EU establishment. Accordingly, Sir Daniel has an existing EU data privacy notice on his website at <https://www.20essexst.com/sites/default/files/privacy/daniel-bethlehem-privacy.pdf>.⁵
- 9) In that data privacy notice, Sir Daniel confirms that the GDPR covers him and that he is both a data “processor” and a data “controller,” as that term is defined in the GDPR.⁶

2. THE OTHER TRIBUNAL MEMBERS

- 10) The other members of the Tribunal reside outside of the EU. Specifically, the President, Cavinder Bull, lives in Singapore and practices law at Drew & Napier, and Doak Bishop lives in Houston, Texas and is a partner of the law firm, King & Spalding, which has three offices in the EU.
- 11) While Arbitrators Bull and Bishop are not EU residents, they may still be covered by the terms of the GDPR if either or both have “stable arrangements” with the EU that may make them subject to the GDPR.

² General Data Protection Regulation, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, art 3(1) (“GDPR”) (*CLA-34*).

³ GDPR art 3(2) (*CLA-34*).

⁴ GDPR art 3(2) (*CLA-34*).

⁵ GDPR Privacy Notice from D. Bethlehem QC website (*C-13*).

⁶ GDPR art 4(7) (*CLA-34*).

- 12) In any event, these two arbitrators will sit on the Tribunal with Sir Daniel Bethlehem. In making decisions together based on evidence submitted by the parties, all three will be jointly “controlling” and “processing” “personal data” as defined in the GDPR. As noted by the Investor in its previous submissions, this concerted activity makes all three subject to the GDPR to the extent that Arbitrators Bull and Bishop are considered “joint processors” and “joint controllers” of data.
- 13) The three arbitrators will likely receive significant amounts of data in the case and will need to “process” (e.g., store and review) that data to make their determination in this matter. Accordingly, throughout this arbitration, all members of the Tribunal may be considered joint controllers of that data. The ICCA-IBA Task Force Report notes that “joint control has been very broadly defined and carries joint and several liability.”⁷
- 14) In addition to possession and review, the GDPR, by its terms, covers any further transfer or disclosure of documents that name or identify any natural persons or have other personal data.

II. TERRITORIAL SCOPE

- 15) The European Data Protection Board (“EDPB”) is empowered to issue guidelines, recommendations, and best practices to encourage consistent application of the GDPR and setting of administrative fines.
- 16) In 2018, the EDPB issued a consultation paper on the territorial scope of the GDPR. It made clear that the GDPR can extend to data processing that occurs outside of the EU:

The text of Article 3(1) does not restrict the application of the GDPR to the processing of personal data of individuals who are in the Union. The EDPB, therefore, considers that any personal data processing in the context of the activities of an establishment of a controller or processor in the Union would fall under the scope of the GDPR, regardless of the location or the nationality of the data subject whose personal data are being processed. This approach is supported by Recital 14 of the GDPR which states that “[t]he protection afforded by this Regulation should apply to natural persons, whatever their nationality or place of residence, in relation to the processing of their personal data.”⁸

- 17) If that data processing occurs in the context of “stable arrangements” with an EU establishment, then it falls within the scope of the GDPR:

⁵ IBA - ICCA Roadmap Annexes – Annex 2 under “Am I a data controller, processor or joint controller?” (C-4).

⁸ European Data Protection Board, Guidelines 3/2018 on the Territorial Scope of the GDPR (Article 3) - at page 9 (CLA-36).

Once it is concluded that a controller or processor is established in the EU, an in concreto analysis should then follow to determine whether the processing is carried out in the context of the activities of this establishment, in order to determine whether Article 3(1) applies. If a controller or processor established outside the Union exercises “a real and effective activity - even a minimal one” - through “stable arrangements”, regardless of its legal form (e.g. subsidiary, branch, office...), in the territory of a Member State, this controller or processor can be considered to have an establishment in that Member State.⁹ It is therefore important to consider whether the processing of personal data takes place “in the context of the activities of” such an establishment¹⁰ as highlighted in Recital.¹¹

- 18) GDPR Articles 1 and 2 indicate that the data privacy regime protects “natural persons,” which is broader than just EU data subjects. Likewise, the definition of “personal data” in Article 4 is not limited to EU data subjects. GDPR Article 3, which describes the territorial scope, says that it applies to EU data subjects when the controller or processor is not established in the EU, but under Article 3(1) there is no limitation to EU data subjects when the Processor or Controller are established in the EU. As a result, the territorial scope covers all natural persons, whether EU data subjects or otherwise. This applies potentially to any person mentioned in, or who can be identified in, any document sent to or from anyone with an EU establishment (like Arbitrator Bethlehem or any other arbitration participant subject to the GDPR).
- 19) The only limitation seems to be some nexus or basis for the application of EU law—*either* an establishment within the EU by those processing or controlling personal data of natural persons *or* the handling of personal data of EU data subjects (or both).

⁹ See in particular para 29 of the *Weltimmo* judgment: *Weltimmo s. r. o. v Nemzeti*, Case C-230/14, Judgement 1 Oct 2015 (CLA-35), which emphasizes a flexible definition of the concept of ‘establishment’ and clarifies that ‘the degree of stability of the arrangements and the effective exercise of activities in that other Member State must be interpreted in the light of the specific nature of the economic activities and the provision of services concerned.’ as referenced at footnote 22 of the European Data Protection Board, Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) (CLA-36).

¹⁰ *Weltimmo s. r. o. v Nemzeti*, Case C-230/14, Judgement 1 Oct 2015, ¶ 25 (CLA-35) and *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, Judgment of the Court (Grand Chamber), 13 May 2014, ¶ 53 (CLA-37), as referenced in the European Data Protection Board, Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) at footnote 23 (CLA-36).

¹¹ European Data Protection Board, Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) - at page 6 (CLA-36).

III. MATERIAL SCOPE

- 20) The Tribunal has enquired about the applicability of Article 2(2)(a) of the GDPR, which provides that the GDPR “does not apply to the processing of personal data ... in the course of an activity which falls outside the scope of [EU] law.”
- 21) First, it must be understood that Article 2 relates to the “material scope” of the GDPR; article 3 relates to its “territorial scope.” Activities that fall outside of the EU territory do not necessarily fall outside of the scope of EU law.
- 22) Secondly, as discussed above, the GDPR applies to the processing of personal data by “establishments.” Article 2 operates to exempt certain types of *non-commercial* data from the scope of the GDPR—including that done by States,¹² ordinary citizens in the course of their household activities,¹³ or “competent authorities” for police investigations or the protection of national security.¹⁴ Arbitration does not fall outside the scope of EU law.
- 23) Setting that aside, it is also clear that a situation in which data from EU sources are shared with a joint enterprise in which at least one member (and maybe more) has an establishment in the EU will fall within the scope of EU law. Thus, Article 2(2)(a) is inapplicable to the case at hand.

IV. THE ROLE OF THE PCA

- 24) The arbitration is being administered by the International Bureau of the Permanent Court of Arbitration (“the PCA”), a supranational organization established under the Treaty on the Pacific Settlement of International Disputes in 1899 (“1899 Hague Convention”) and the Treaty on the Pacific Settlement of International Disputes in 1907 (“1907 Hague Convention”) and seated at The Hague, Netherlands, pursuant to those treaties¹⁵
- 25) Article 24 of the 1899 Hague Convention and Article 46 of the 1907 Hague Convention establishes diplomatic privileges and immunities for the Members of the Permanent Court of Arbitration when they are acting as arbitrators—but these treaty provisions are inapplicable to the case at hand. This is a NAFTA arbitration governed by the 1976

¹² GDPR art 2(2)(b).

¹³ GDPR art 2(2)(c).

¹⁴ GDPR art 2(2)(d).

¹⁵ The Hague Convention for the Pacific Settlement of Disputes 1899 (“1899 Hague Convention”) art 22(1) (*CLA-38*); The Hague Convention for the Pacific Settlement of International Disputes of 1907 (“1907 Hague Convention”) art 43 (*CLA-39*)

UNCITRAL Rules of Arbitration, and the members of the Tribunal are not Members of the Permanent Court of Arbitration. The PCA is only acting as Administrator.

- 26) The PCA has a headquarters agreement with the Netherlands that governs the relationship between the two parties, i.e., Agreement Concerning the Headquarters of the Permanent Court of Arbitration (“PCA Headquarters Agreement”).¹⁶ However, unlike the 1899 Hague Convention and the 1907 Hague Convention, the PCA Headquarters Agreement is not an international treaty.
- 27) Article III (2) of the PCA Headquarters Agreement renders the PCA and its property inviolable to actions brought in the Netherlands:

*The Headquarters of the PCA shall be inviolable. The Property of the PCA, wherever situated, shall be immune from search, requisition, confiscation, expropriation and any other form of interference, whether by executive, administrative, judicial or legislative action except in so far as the PCA shall have expressly waived its immunity. It is, however, understood that no waiver of immunity shall extend to any measure of execution.*¹⁷

- 28) The term, “Headquarters”, is defined in the following way:

“Headquarters” shall mean the area and any building, including conference facilities, parts of buildings, land or facilities ancillary thereto, irrespective of ownership, used by the PCA on a permanent basis or from time to time, to carry out official functions.

- 29) Because the PCA Headquarters Agreement is, at its core, a contract between the Netherlands and the PCA, it has no effect outside of the Netherlands.
- 30) The Investor is unaware of any agreement directly between the PCA and the EU. It is aware, however, of “host country agreements” that the PCA has negotiated with other EU countries, like Portugal and Ireland.¹⁸ Those agreements specifically provide that the PCA “shall enjoy immunity from every form of legal process except insofar as in any particular case it has expressly waived its immunity.”¹⁹

¹⁶ Agreement concerning the Headquarters of the Permanent Court of Arbitration, March 30, 1999 (“PCA Headquarters Agreement”) (*CLA-40*).

¹⁷ PCA Headquarters Agreement at Article III (2) (*CLA-40*).

¹⁸ “Host Country Agreements,” webpage on Permanent Court of Arbitration Website (*C-15*). Available at <https://pca-cpa.org/en/relations/host-country-agreements/>

¹⁹ See, e.g., Host State Agreement Between the Portuguese Republic and the Permanent Court of Arbitration, art 9(1). (*CLA-43*); The Host Country Agreement between the PCA and the Republic of Ireland is not publicly available.

- 31) The presence of these host country agreements and the privileges and immunities clauses therein suggest that the inviolability of the PCA only applies to acts within the territory of the Kingdom of the Netherlands and those EU countries with which the PCA has host country agreements, *i.e.*, Portugal and Ireland.
- 32) Furthermore, the PCA is not exempt from EU law. Instead, the PCA is considered a supranational institution under EU data protection law, and data transfers between itself and others in and out of the EU are considered international transfers.
- 33) Consequently, as discussed in the Investor’s earlier April 16 and April 23 submissions, GDPR obligations will arise whenever there is a “data transfer” occurring between the PCA and the Tribunal. Thus, the Tribunal needs to ensure that data privacy is maintained and the GDPR is followed whenever those data transfers occur.

3. IMPACT OF THE HEADQUARTERS AGREEMENT ON TRIBUNAL MEMBERS

- 34) Members of the Permanent Court of Arbitration who are chosen as arbitrators in a PCA arbitration are classified as PCA Adjudicators under Article 1(8) of the PCA Headquarters Agreement, and under Article 9 of that same agreement, considered to be “diplomatic agents” under the 1961 Vienna Convention on Diplomatic Affairs.
- 35) This is not a PCA arbitration, however. This arbitration arises under the NAFTA and the 1976 UNCITRAL Arbitration Rules. The decision of the parties to use the International Bureau as an administrating authority does not change that fact. The International Bureau and the Court are separate entities.²⁰
- 36) Unfortunately, neither the NAFTA nor the 1976 UNCITRAL Arbitration Rules confer diplomatic immunity from national law on arbitrators. Therefore, the members of the Tribunal are subject to the terms of the GDPR as much as they otherwise would be.

4. NON-DISPUTING PARTIES UNDER THE TREATY

- 37) Under the NAFTA, the governments of Mexico and the United States are entitled to receive the evidence submitted in this arbitration, provided that they receive it subject to the same obligations as one of the parties.
- 38) Specifically, NAFTA Article 1129 states:

²⁰ “About Us” webpage on Permanent Court of Arbitration Website (*C-16*), available at <https://pca-cpa.org/en/about/>.

Article 1129: Documents

1. A Party shall be entitled to receive from the disputing Party, at the cost of the requesting Party a copy of:

(a) the evidence that has been tendered to the Tribunal; and

(b) the written argument of the disputing parties.

2. A Party receiving information pursuant to paragraph 1 shall treat the information as if it were a disputing Party.²¹

39) In accordance with these provisions, if Mexico and the United States requested the evidence and submissions in this arbitration from Canada, they would be required to comply with the same rules imposed upon Canada

40) This Tribunal has expanded the conditions for disclosure of materials to Mexico and the United States beyond that contemplated by NAFTA Article 1129. Section 11.1 of Procedural Order No. 1 reads:

*The Governments of Mexico and the United States may attend hearings and make submissions to the Tribunal within the meaning of Article 1128 of the NAFTA by the dates to be determined in the Procedural Calendar. **They shall be entitled to receive a copy of the confidential versions of evidence and submissions referred to in Article 1129 of the NAFTA.**²²*

41) If Mexico and the United States obtain confidential evidence directly from the Tribunal or the Investor, then the GDPR would apply—and there would be a requirement to ensure that those two States applied the terms of the GDPR. However, the Tribunal does not have the authority to impose an order of GDPR compliance against Mexico and the United States, as they are not parties to this arbitration.

42) Moreover, as any disclosure by the Tribunal or Investor would not occur via the process contemplated by NAFTA Article 1129, the protections of Article 1129(2) would not be applicable—and the data transfer could lead to GDPR liability for the Tribunal in the event of non-compliance by Mexico and the United States.

43) There is a solution to this issue. Should the data transfers to Mexico and the United States occur under the process set out in NAFTA Article 1129(2), then they would sit outside of

²¹ NAFTA Article 1129 (CLA-42).

²² Procedural Order No. 1 at § 11.1.

the Tribunal and the PCA. The NAFTA would govern, and such a transfer by Canada in North America would be outside the terms of the GDPR.

V. SPECIFIC ANSWERS

Question 1 - Could you please address the applicability of the GDPR to the proceedings in question, having regard to Article 2(2)(a) of the GDPR – which provides: “This Regulation does not apply to the processing of personal data (a) in the course of an activity which falls outside the scope of Union law” – and that the arbitration is governed by the NAFTA, a treaty to which neither the EU nor any of its Member States are a party, is between two non-EU parties, and is not governed or otherwise subject to or within the scope of either EU law or the law of any EU Member State.

Answer to Question 1 - Scope

- 44) As explained above, GDPR Article 2(2)(a) is not relevant to the questions before the Tribunal as this is a matter that falls within the scope of EU law. The situation referenced in Article 2(2) applies to categories of information that are not covered by EU law, like personal data used for household use or personal data used in police investigations. Personal data transferred for commercial purposes, such as for an arbitration practice or the administration of arbitration, is an area subject to EU law—and thus Article 2(2) applies.
- 45) In the Tribunal’s communication of May 16, 2019, the Secretary stated that:
- Separately, the Tribunal considers that since it is the Claimant who has raised the GDPR as an issue to be addressed in this proceeding, the onus lies on the Claimant to initiate whatever processes it deems necessary to propose a Data Protection Protocol for the Tribunal’s consideration.²³
- 46) The Investor respectfully notes that the responsibility to ensure that the Tribunal acts lawfully does not fall upon the Investor. That obligation is for the Tribunal to discharge.
- 47) This is a dispute involving a non-EU treaty, i.e., the NAFTA, and the Investor wishes that it did not have to raise these issues. It neither seeks to have EU law applied in this case nor advocates for a broad application of the GDPR. But it felt that it had a duty to bring these regulatory issues to the Tribunal’s attention, so the Tribunal could establish a compliance process that is lawful, effective, and efficient.
- 48) Neither the parties nor the Tribunal bears responsibility for the EU having enacted the GDPR—a regulation of general effect that is both broad in scope and vague in its limits. Nevertheless, the arbitration participants must now work together to establish a process to address issues raised by the GDPR—as onerous as this may be for all concerned—to

²³ Email from C. Tham to disputing parties - May 16, 2019 (C-14).

maximize compliance and minimize the risk of any liability being imposed on the parties or the Tribunal.

Question 2 – the PCA Headquarters Agreement - Could you please address the applicability of the GDPR to the PCA, having regard, *inter alia*, to The Netherlands-PCA Headquarters Agreement, which provides, *inter alia*, in Article 9(1), that “PCA Adjudicators” (which includes arbitrators taking part in a hearing, meeting or other activity in relation to PCA Proceedings; which is in turn broadly defined) “shall, in the exercise of their duties, enjoy such immunities as are accorded to diplomatic agents pursuant to the Vienna Convention [on Diplomatic Relations].” Amongst the extensive immunities accorded to diplomatic agents are, *inter alia* (a) immunities from civil and administrative jurisdiction, save in respect of very limited exceptions, (b) a privilege against giving evidence as a witness, (c) the inviolability of papers, correspondence and (subject to limited exception) property, and (d) immunity from execution. As the Tribunal reads these provisions, their effect would be to preclude suit before the Dutch courts against a tribunal or an individual arbitrator seeking to obtain papers relating to the arbitration, including going not only to deliberations but also any other case papers, and including those relating to data subjects. While the question remains as to the weight that would be accorded to the HQA in the case of proceedings before the courts of other States, such courts may be expected to have careful regard to the HQA in the case of any such proceedings.

Answer to Question 2

- 49) As discussed more fully above, the PCA Headquarters Agreement does not provide a dispensation from the GDPR. While it provides a number of legal protections—including immunity from Dutch law and the promise of diplomatic assistance from the Netherlands in dealing with other States—it does not grant the Administrator immunity from EU law.
- 50) The PCA Headquarters Agreement is not at all applicable to the Tribunal, as they are not PCA Adjudicators. Moreover, as set out in prior submissions to the Tribunal, the Data Protection Authorities in the UK have explicitly stated that they will not exempt arbitrators from the requirements of the GDPR.

Question 3 – Data Privacy Notice

- 51) The Tribunal has provided the Investor with a copy of the data privacy notice issued by Sir Daniel Bethlehem. The Tribunal sent the following comment:

This Privacy Notice, which has been publicly exhibited since the entry into force of the GDPR, reflects considered advice on GDPR compliance.

As regards both systems and procedures, the arrangements in place in respect of Arbitrator Bethlehem’s professional

activities, including in respect of arbitration proceedings, are considered to be GDPR compliant.²⁴

- 52) A data privacy notice is a requirement for the handling of personal data, but it does not constitute the full extent of what is required to be compliant with the GDPR. It is simply one of several steps.
- 53) A data privacy notice needs to be seen by the natural persons identified, or who could be identified, in documents processed and transferred across borders in connection with this arbitration. Affirmative steps are required to provide GDPR-compliant notices to those data subjects to the extent practical.
- 54) The Tribunal will also be data controllers and data processors under the terms of the GDPR, so will also be required to take affirmative steps for GDPR compliance. The Investor cannot assess what other steps the Tribunal and Administrator might have to take to be compliant with the GDPR without receiving answers to the questions in Appendix A.
- 55) Furthermore, the PCA may need to take separate measures depending on how it handles the data and website for this arbitration.
- 56) The remaining arbitration participants would also need to take steps to ensure compliance.
- 57) None of these matters are answered by the data privacy notice provided by Sir Daniel. These other issues go to matters outside the scope of a data privacy notice.
- 58) The Investor suggests that it would be beneficial to include a discussion of these matters at the upcoming procedural meeting to see if there are some simple ways to address them.

Submitted on June 4, 2019, on behalf of Counsel for the Investor.



Barry Appleton

²⁴ Email from C. Tham to disputing parties - May 28, 2019 (C-12).

QUESTIONS FOR THE TRIBUNAL

All terms used in these questions refer to the meaning in the GDPR and as discussed in the Investor’s Submissions and supporting materials to it.

1. ARBITRATOR SPECIFIC QUESTIONS

- 1) Sir Daniel’s Data Privacy Notice discloses that data is moved from the UK to Singapore. Can Sir Daniel please describe where data for this arbitration will be stored and the circumstances which would necessitate the transfer of data outside of the EU?
- 2) Can Sir Daniel explain if he engages in co-located servers storing personal data? If so, where are these servers physically located? Which servers would be used for data involved in this arbitration?
- 3) Can President Bull describe whether he has a permanent establishment or “stable arrangements” in the EU? When answering this question, please include any door tenancies or other relationships.
- 4) Does Drew & Napier have a permanent relation or “stable arrangements” in the EU?
- 5) Does Drew & Napier target data subjects in the EU in any manner, such as offering services to any persons in the EU?
- 6) Does President Bull or Drew and Napier have co-located servers storing personal data? If so, where are these servers physically located? Which servers would be used for data involved in this arbitration?
- 7) Does Arbitrator Bishop have a permanent establishment or “stable arrangements” in the EU? When answering this question, please include any door tenancies or other relationships.
- 8) Does King & Spalding have “stable arrangements” in the EU?
- 9) Does King & Spalding target data subjects in the EU in any manner, such as offering services to any persons in the EU?
- 10) Does King & Spalding engage in co-located servers storing personal data? If so, where are these servers physically located? Which servers would be used for data involved in this arbitration?

2. GENERAL QUESTIONS FOR THE TRIBUNAL

- 11) The “purpose limitation” for data means that data is only used for the purposes for which it was originally collected and for specific and limited purposes that need to be communicated to the data subjects. Does the Tribunal have any process in place to provide data subject notices?
- 12) Can each member of the Tribunal please describe the data protection practices that they have in in place (or will be putting into place) for each location where they may store or access personal data for this Arbitration, including but not limited to cyber breach protection?
- 13) Does the Tribunal have an approach in mind to address the content of data privacy notices? Would this include a mandate that data privacy notices are posted by the Tribunal, disputing parties, the PCA and all affected arbitration participants?
- 14) Will the Tribunal ever engage in deliberations on this claim in Europe other than in the territory covered by the PCA Headquarters Agreement?
- 15) Data minimization procedures may be required for GDPR compliance, to reduce the volume of personal data processed and/or transferred. Such steps could also reduce administrative burden and cost in this arbitration. Has the Tribunal considered data minimization steps it could apply in light of the principles in Article 5 of the GDPR?
- 16) Can you describe how evidence and deliberative materials based on evidence containing personal data provided to the Tribunal will be:
 - a) Handled;
 - b) Considered;
 - c) Made public;
 - d) Stored in a manner that protects against accidental loss, destruction or damage;
and
 - e) Eventually destroyed
- 17) There needs to be a basis for a lawful transfer of data between the Tribunal, the PCA, or any person assisting the Tribunal. Are any procedures in place to address evidence containing personal data, and deliberative materials based on that evidence, for each of the steps outlined in sub-paragraphs a to e of question 16 above?

- 18) What steps have been put in place, or can be put in place, for persons accessing personal data in this arbitration such as administrative assistants assisting the tribunal?

3. THE PCA

- 19) Can you please answer the following questions:
- a) Are arbitrators appointed under the provisions of the North American Free Trade Agreement PCA Adjudicators simply because of the administration of a case by the PCA? If so, can you please explain exactly how this status is conferred in this arbitration claim?
 - b) Does the PCA have an agreement or MOU with the EU or an EU Data Protection Authority providing the PCA with an express exemption from compliance with the GDPR? If so, can you provide a copy of this document?
- 20) Is the PCA targeting data subjects in the EU in any manner, such as offering services to any persons in the EU?
- 21) Data storage or Transfers outside of the territory covered by the Headquarters Agreement affect GDPR compliance. Can you please answer the following questions?:
- a) Can the Permanent Court of Arbitration confirm whether data sent or maintained by the PCA for this arbitration is stored and processed entirely on premises that are subject to the PCA Headquarters Agreement?
 - b) Does the PCA use co-located servers? If so, where are they physically located? Which servers would be used for data involved in this arbitration?
 - c) The PCA usually creates a web-based repository for publication of data on the internet. Where are the servers and the data physically located?
 - d) The PCA also has a web server to store evidence. Where is this physically located?
 - e) The PCA will be collecting physical evidence. GDPR also covers it. Where will these records be physically located?
 - f) Can you describe how evidence and deliberative materials based on evidence containing personal data provided to the Tribunal will be:
 - i) Handled;
 - ii) Considered;
 - iii) Made public;

- iv) Stored in a manner that protects against accidental loss, destruction or damage; and
 - v) Eventually destroyed
- 22) There needs to be a basis for a lawful transfer of data between the PCA and the Tribunal and there needs to be a basis for a lawful transfer of data between the PCA and any person working for the PCA that is not covered by the Headquarters Agreement. This would apply to data stored outside of the Netherlands or by someone who is not part of the Permanent Court of Arbitration (such as a third-party provider). What procedures are in place or can be set up to address evidence and deliberative materials based on evidence containing personal data provided to the Tribunal as described in paragraph(f)(i) to (v) of Question 21 above?
- 23) What steps have you put in place, or can be put in place, for persons accessing or otherwise processing personal data in this arbitration such as transcriptionists and administrative assistants assisting the tribunal?

VI. CANADA

- 24) For GDPR classification, can the Government of Canada confirm whether Canada and the province of Ontario have permanent establishments in the EU? Please identify permanent offices or other establishments that the Government of Canada and the province of Ontario have in the EU? Please, identify the city, the office or establishment, and its purpose. In the response, please include consular, tourism, cultural and commercial operations of the Government of Canada and the Government of Ontario.
- 25) Outside of those permanent offices or locations, does the Government of Canada or the Government of Ontario have a “stable relationship” in the EU? If so, please describe the nature of the stable arrangement.
- 26) Is Canada targeting data subjects in the EU in any manner, such as offering services or promoting tourism in Canada to any persons in the EU?
- 27) Is the province of Ontario targeting data subjects in the EU in any manner, such as offering services, or promoting tourism in Ontario to any persons in the EU?
- 28) Has Canada engaged counsel or experts who would trigger GDPR requirements? If so, what procedures have been put into place for GDPR compliance?
- 29) Does Canada envision engaging witnesses who would trigger GDPR requirements in Europe? If so, what procedures have been put into place for GDPR compliance?

30) The EU has only permitted the transfer of data to commercial organizations in Canada. The EU determined that Canada's *Personal Information Protection and Electronic Documents Act* (PIPEDA) was providing adequate privacy protection. PIPEDA only applies to private sector companies and expressly does not apply to the Government of Canada and provincial governments. Since the Government of Canada is not covered by PIPEDA, data transfers to the Government of Canada do not have Adequacy Decision coverage, and safeguards are required. In light of the absence of an applicable adequacy decision, can Canada describe how evidence containing personal data will be:

- a) Handled;
- b) Considered;
- c) Made Public;
- d) Stored in a manner that protects against accidental loss, destruction or damage;
and
- e) Eventually destroyed.