From: Barry Appleton
Sent: 17/04/2019 04:01:39

BCC:
Subject: Investor comments on the EU General Data Privacy Regulation; - Tennant Energy, LLC (U.S.A.) v. Government of Canada

The Investor writes further to the April 10, 2019 direction of the Tribunal concerning the issue of Data Privacy, data protection and cybersecurity. As outlined below, significant issues arise in connection with data privacy and security which merit a comprehensive discussion of the parties, secretariat and disputings parties as early as possible.

The Investor suggests that careful attention should be paid to the policy of data minimization under the EU General Data Privacy Regulation ("GDPR"), which is relevant to our arbitration as a result of having an arbitrator in a European state. (By the term GDPR, the Investor is referring to 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 the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016, p. 1.)

Any personal data information coming from or going to Sir Daniel Bethlehem in this arbitration is governed by the GDPR and creates GDPR liability. Furthermore, any deliberations that take place electronically with Sir Daniel in the United Kingdom could be governed by the GDPR for at least a period (depending on the outcome of negotiations between the United Kingdom and the European Union concerning the former's withdrawal from the latter).

We understand that the PCA is exempt from the GDPR, due to its status as a supranational organization. In the words of the IBA Roadmap:

> In the arbitration context, it is important to recall that international organisations 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, are treated as though they are outside the EU (Art. 4(26) defining international organisations, Art. 46(1) addressing transfers to international organisations). This means that transfer to such organizations will require compliance with the data transfer rules.

Because of the exemption, any protected data that crosses an "international frontier" every time it transfers between Sir Daniel and the PCA. This is the same with any covered data transmitted by Sir Daniel to the other arbitrators. This all triggers GDPR obligations. As a result, data processing and privacy require discussion.

The penalties for non-compliance on Arbitrator Bethlehem are significant. They include criminal penalties, and they create joint and several liability. The Investor notes that the indemnity provisions in Article 11 of the Terms of Appointment do not apply to this type of liability. Furthermore, there can be judicial measures applied in the EU that could detrimentally affect the operation of this arbitration under the North American Free Trade Agreement. IBA-ICCA notes that non-compliance with the GDPR may also be relevant to objections to the enforceability of an award issued by the Tribunal.

The process regarding the treatment and processing of confidential information is highly relevant to the obligations in the GDPR. As a result, it is essential that the Confidentiality process is decided in a manner consistent with the GDPR. It is for that reason that the Investor requests that a data privacy and security discussion occur with the Tribunal and the disputing parties in person.

The Investor notes that the International Bar Association (IBA) and the International Council of Commercial Arbitration (ICCA) has struck a task force to assist tribunals with addressing this very issue. One of the lead counsels for the Investor has had an opportunity to be involved in the consultation process regarding the joint IBA-ICCA Taskforce on Data Privacy in International Arbitration.

The Task Force has not yet issued its report, but it has crafted a significant document on Data Privacy. We have enclosed the draft report, its draft Annexes and the Draft RoadMap to assist the Tribunal and the disputing parties with this very important issue. We note that the Roadmap is particularly helpful.

We note the following extract from page (i) of the introduction to the Roadmap issued by the Task Force. It states:

> **a. Why should you care?**
>
> Every participant in an arbitration who has access to personal data (including the parties, their counsel, arbitral institutions, arbitrators, experts, vendors and service providers (e-discovery experts, information technology professionals, court reporters, translation services, etc.) referred to as "**Arbitral Participants**") should consider for each individual case whether any data protection laws may apply and if so, what that means for them and for the conduct of the arbitration.

Page 18 of the IBA-ICCA RoadMap states:

> After the arbitral tribunal is constituted, the parties and arbitrators can also raise any data protection issues directly with each other. If data protection has not already been addressed or fully addressed, it is good practice to include the topic on the agenda of the Case Management Conference or first procedural meeting and address the relevant issues at that occasion. This will allow the parties, counsel and the tribunal (where

necessary in conjunction with the institution) to consider at the outset of the proceedings how the applicable data protection regime(s) will play out in the context of that particular arbitration. Additional complications may arise with defaulting parties.

Also, ICCA, the City Bar of New York, and the International Institute for Conflict Prevention and Resolution ("CPR") have issued a Draft Cybersecurity Protocol for International Arbitration. A copy of this draft is attached.

We have enclosed a link to an excellent short article on the subject issued by Markus Burianski at White & Case
https://www.whitecase.com/publications/alert/data-privacy-international-arbitration

While there is a court exception, as noted in the IBA-ICCA Report, Advisory Decision 26 confirms that there are no exceptions to the reach of the GDPR applicable to arbitration. Furthermore, under the GDPR, data transfers to supranational organizations such as the Permanent Court of Arbitration, even though located in the EU, are treated as an export of data from the EU. As a result, the GDPR rules are triggered every time there is a transmission to or from the PCA to the Tribunal or from the disputing parties to the Tribunal.

***GDPR***

Because of the large definition of personal data witness statement would be covered by the GDPR. For example, the definition of "personal data" under the GDPR would include the names of the witness', their address, their birthdates and evidence provided by them.

The arbitrators and PCA, are considered as "processors" of the information under the GDPR. The term p**rocessing'** means any operation or set of operations which is performed on personal data or sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

A **'processor'** means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

The Tribunal process personal data when it reviews evidence or makes a decision. The PCA is processing data when it collects, stores or transmits data. The disputing parties, party witnesses and experts may all fit within the category of "joint controllers" under the GDPR.

As a result, there must be a proper GDPR compliance mechanism in place.

One GDPR core principle, enshrined in Article 5 of that regulation, is data minimization. Article 5 is the starting point for the processing of personal data generally and sets out the general principles upon which the GDPR is based. Article 5(c) sets out the principle on data minimization, which states that personal data shall be:

> (c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimization');

This principle is inextricably interconnected with the Tribunal's approach to the treatment of confidential data.

***Definitions***

- **'personal data'** means any information relating to an identified or identifiable natural person ('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 to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person**;

- '**controller**' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

- personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

***General***

The starting point for any data processing is compliance with the following principles (Art. 5 GDPR). These principles have some similarity to those under the EU Data Protection Act but there are differences and also new concepts: 5(1) Personal data shall be: -

> (a) **processed lawfully,** fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');
>
> (b) **collected for specified, explicit and legitimate purposes** and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical

purposes shall, in accordance with Art. 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');

(c) **adequate, relevant and limited to what is necessary** in relation to the purposes for which they are processed ('data minimisation');

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay

(e) **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**; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Art. 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');

(f) **processed in a manner that ensures appropriate security of the personal data**, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

5(2) The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').

In the words of the IBA- ICCA RoadMap:

> The GDPR requires all Arbitral Participants, including both data processors and data controllers, **to apply adequate physical and cyber security whenever they process personal data, failing which they risk fines and other enforcement action**.
>
> The GDPR requires **data controllers and processors to implement appropriate technical and organisational measures** to ensure a "*level of security appropriate to the risk*" (Art. 32). This means that whenever the GDPR applies to personal data processed in an arbitration, adequate data security is *mandatory*. However, the GDPR does not define the security measures that are required for compliance.
>
> Article 5(1)(f) of the GDPR concerns the "*integrity and confidentiality*" of personal data. It establishes the principle that personal data shall be "*processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures*." *(emphasis added*)

The Tribunal will need to address each of these obligations. In so doing, it will need to work

with the disputing parties to ensure that the approach taken is not overly burdensome to the arbitration.
In general, in the words of the ICCA- City Bar -CPR "Draft Cybersecurity Protocol":

> Parties expect that the providers of dispute resolution services and other participants in the dispute resolution process will take reasonable measures to protect non-public exchanges of information, including reasonable cybersecurity measures, to safeguard digital information from unauthorized access and disclosure

The Tribunal will also need to address data notification requirements. These are now essential under the GDPR. The IBA – ICCA RoadMap introduces this topic as follows:

> Unless an exemption applies, the GDPR requires data privacy notices to be provided both by the data controller that originally collects the personal data from the data subject, and by those that receive the personal data subsequently. Most Arbitral Participants fall in the second category. This means that unless exempted, each of the Arbitral Participants will need to provide a notice to all data subjects whose personal data is processed during an arbitration.

The notification process for processing and about data breach (another key obligation) is essential. There appears to be no way around this requirement.

**Next Steps consideration for the Tribunal**

**There are currently no provisions in the Terms of Appointment nor in Procedural Order No. 1 that address any of these issues.** The issue of data privacy and security is complicated. This is a matter that requires collaboration and discussion with all interested parties.

The Investor recognizes that there would be an opportunity to discuss these matters with the entire Tribunal at the First Procedural Meeting. For the reasons outlined above, a frank discussion at the outset of the arbitration is essential.

The Investor notes that it is important to design a process that avoids the necessity to obtain consent from those who provide information. Under the GDPR, such consents may be withdrawn at any time and thus leave the Tribunal and parties highly vulnerable to not being able to consider essential, necessary and material evidence.

The Investor suggests that the following be developed:

- A data protection protocol which could be issued as a subsequent procedural order that would cover data protection and notification, data subject rights, data breach and on cybersecurity;
- That the Tribunal issue in Procedural Order No 1 its authority to determine what security measures, if any, are reasonable in the circumstances of the case, taking into account the

views of the parties (and the other Arbitral Participants, to the extent the tribunal considers to be appropriate) and to order the implementation of such measures.

- An agreed approach to address the protection and reception of evidence;
- Agreement on Data minimization, Redaction and encryption procedures for personal data;
- An approach to address to reduce the risk of information data breach in Tribunal's orders or awards.

Accordingly, the Investor seeks to obtain comments from the Respondent, the Tribunal and the Permanent Court of Arbitration to be able to jointly develop procedures to address the data privacy and security issues in this arbitration.

Submitted on behalf of counsel for the Investor,

**Barry Appleton**
*Managing Partner*
*Appleton & Associates International Lawyers LP*
Tel 416.966.8800 • Fax 416.966.8801
bappleton@appletonlaw.com • www.appletonlaw.com
77 Bloor St. W, Suite 1800, Toronto, Ontario • M5S 1M2