CIArb
evolving to resolve
Singapore Branch

THE CHARTERED INSTITUTE OF ARBITRATORS
SINGAPORE BRANCH

COMPETITION 2019

COMPETITION PACK

Amended as of 14 OCTOBER 2019
SINGAPORE

Supported by: TAC THE ARBITRATION CHAMBERS ARBITRATORS & MEDIATORS

AFIA ASIA-PACIFIC FORUM FOR INTERNATIONAL ARBITRATION

Contents

Competition Pack 2019
Singapore

SECTION A. RULES OF COMPETITION

SECTION B. ARBITRATION PAPERS

Supported by: TAC THE ARBITRATION CHAMBERS ARBITRATORS & MEDIATORS AFIA ASIA-PACIFIC FORUM FOR INTERNATIONAL ARBITRATION

Section A:
Rules of Competition

CIArb
evolving to resolve

Competition Pack 2019
Singapore

1. Background

The Chartered Institute of Arbitrators (Singapore branch) Competition for 2019 concerns issues of personal privacy, data protection and cybersecurity in international arbitration. It considers the potential extra-territorial reach of data protection legislation and how that may affect the conduct of international arbitration.

2. Competition Submission

The factual scenario used in the competition, including all people, companies, locations and events, is fictional. Any resemblance to actual persons, places or events is unintended and coincidental.

You are the chair of the tribunal in an ad hoc arbitration. The parties are a US incorporated sovereign wealth fund of a fictitious EU member-state and a Singaporean software development company. The dispute arises out of the development of an online software platform which harvests its participants' sensitive personal data using wearable technology. The participants of the platform are citizens and residents of the EU. There are allegations that the platform has been hacked and that, inter alia, the (sensitive) personal data of the participants have been stolen. The parties disagree as to the applicability of the EU General Data Protection Regulation ("**GDPR**") to these arbitration proceedings and how it affects a party's right to conduct discovery pursuant to the US Federal Rules of Civil Procedure pursuant to the arbitration clause. Further, due to the background and nature of this dispute, there are also concerns about the appropriate cybersecurity measures to be adopted. Following a second procedural hearing, your co-arbitrators have come to a consensus as to the issues which they consider are raised by the competing submissions. The relevant evidence and notes from the procedural hearing is provided in section B.

As the presiding arbitrator, you have to rule on the procedure to be adopted. You have agreed with your fellow arbitrators that you will prepare a draft order for discussion with them. You also decide to prepare some notes so that you can explain your procedural order and persuade your co-arbitrators to adopt it.

Competitors must submit:
(1) draft procedural order for discussion with your co-arbitrators; and
(2) an explanatory note that sets out the reasoning for making your order.

All submissions must be sent to competition@ciarb.org.sg in the format provided in the rules below. All entries will be anonymised before submission to the judging panel.

Supported by: TAC THE ARBITRATION CHAMBERS ARBITRATORS & MEDIATORS AFIA ASIA-PACIFIC FORUM FOR INTERNATIONAL ARBITRATION

3. Word Limit

There is no word limit for the text of the draft procedural order.

There is a word limit of 3,500 words for the commentary on the procedural order. The commentary may cite legal authorities, published articles and other publicly available materials should you wish.

4. Judging Criteria

Entries will be judged based on:

(1) identification of the pertinent issues affecting procedural aspects of the arbitration;
(2) clarity, conciseness and content of the draft order; and
(3) reasoning in the explanatory note

5. Judging Panel

The judging panel for this Chartered Institute of Arbitrators (Singapore Branch) Competition 2019 comprises of Ms Kathleen Paisley, Partner, Ambos NBGO Advocaten, Mr Andrew Moran QC, Independent Arbitrator, The Arbitration Chambers, Mr Timothy Cooke, Partner, Stephenson Harwood LLP and Mr Shaun Lee, Counsel, Bird & Bird ATMD LLP. Ms Paisley is a task force co-chair on the ICCA-IBA Joint Task Force on Data Protection in International Arbitration Proceedings.

6. Deadline for Submissions

The deadline for submitting entries into the competition is 8 November 2019.

7. Prizes

First Prize Winner: cash prize of S$ S$2,000. The winner will also receive a speaking slot on the panel of a forthcoming CIArb Singapore event on data protection and cybersecurity.

Second Winner: cash prize of S$ S$1,000.

Third Prize Winner: cash prize of S$500.

All cash prizes are generously sponsored by The Arbitration Chambers.

8. Rules

(1) The competition is open to anyone, whether or not they are members of the Chartered Institute of Arbitrators.
(2) The submission must be the original and sole work of the entrant.
(3) Each entrant may only submit one entry.
(4) All entries shall be in English, typed, and submitted in Microsoft Word format. Each entry is to be accompanied by a title page stating the entrant's name, contact details, place of residence, place of work and age.
(5) All entries will be acknowledged but will not be returned. The organisers will accept no responsibility for the safekeeping of entries.
(6) All persons entering the competition agree to allow the Chartered Institute of Arbitrators and the CIArb Singapore Branch to publish any part of any entry submitted for the competition.
(7) The judging panel may in their absolute discretion award each of the prizes to more than one person or award no prizes.
(8) The judging panel's decision shall be final and no correspondence will be entered into.

Supported by: TAC THE ARBITRATION CHAMBERS ARBITRATORS & MEDIATORS AFIA ASIA-PACIFIC FORUM FOR INTERNATIONAL ARBITRATION

Section B: Arbitration Papers

CIArb
evolving to resolve

Competition Pack 2019
Singapore

Statement of Claim

1. SierraWhiskeyFoxtrot LLC ("**SWF**") is the Republic of Otan's state-backed fund that primarily invests into areas of Otanian national interest. At present, this includes areas of national security, healthcare and financial technology ("**FinTech**"). SWF is incorporated in the state of Delaware, United States of America.

2. Otan is a member state of the European Union. For historical reasons, its laws and law-making institutions are identical to those of the laws of England and Wales.

3. Alpha Technology Aggregator System Pte Ltd ("**ATAS**") is a company incorporated under Singapore law which is engaged in the business of software and platform solutions development. It is an award winning technology start-up lauded for its innovative use of big data and proprietary AI systems and other machine learning algorithms that "nudge" its users towards desired outcomes in the health and financial space.

4. Otan's executive has recently launched a 5 year programme to combat high levels of lifestyle chronic diseases like obesity, hypertension and diabetes. Concurrently, there is a separate governmental push to promote Otan as the FinTech centre of Europe.

5. An intermediary known to both ATAS and SWF placed the parties' representatives in contact with one another to discuss possible areas of collaboration. Pursuant to those discussions, ATAS proposed to set up a branch in Otan (the "**Branch**") to develop a customised online platform in which participants on the platform would be rewarded for health conscious behaviour with, inter alia, cash payments into their designated bank accounts (where such information is provided), rebates against their credit card purchases as well as earning virtual currency (the "**Platform**"). The Participants primarily accessed the Platform through a mobile application installed on their personal phones or wearable smart devices.

6. SWF agreed to fund ATAS's development of the Platform. And it was on the basis of the foregoing that parties entered into a Platform Development Agreement dated 8 August 2018 (the "**Agreement**"). The Agreement envisaged that there would be a period of beta-testing prior to the user-acceptance test in or around May to July 2019 and a subsequent "go-live" of the Platform in or around August 2019.

7. SWF accepts that all appropriate and fully informed consents were obtained from the participants in the beta-testing of the Platform (plurally "**Participants**"; singularly "**Participant**"). Due to personal data and Otanian domestic national security concerns, citizens and residents of other EU member-states were specifically

excluded as Participants. SWF was assured by ATAS that this would be achieved through geo-blocking of European IP addresses as well as "Know Your Customer" processes carried out by the Branch's employees.

8. A Participant's personal data (including critical or sensitive personal data such health-related data, genetic data, biometric data as well as financial data) was collected and stored for the purpose of the use of the Platform. In particular, the Participant's financial, behavioural and health related data were harvested through real-time sensors in the form of wearable gear (e.g. fitness trackers or smart watches) or through their mobile phones. For security reasons, the Participant's biometric data in the form of facial recognition, fingerprints and/or iris scans were not only stored on the local device (i.e. the Participant's mobile phone) but also on the Platform's servers.

9. Pursuant to the terms of the Agreement, the parties also agreed that the servers running the Platform and storing the Participants' data would be physically situated in Singapore. The Agreement further provided that ATAS would be responsible for the cybersecurity of the Platform in accordance with any mandatory law which may be applicable. The operative clause reads as follows:

> *"**27 Data Protection and Cybersecurity***
>
> *27.1 ATAS shall be responsible for the collection, use, disclosure and transfer of all personal data pertaining to the Platform which ATAS has or will receive, possess or otherwise have access to.*
>
> *27.2 ATAS further agrees that its collection, access, use, storage, disclosure, transfer and destruction of such personal data shall be in accordance to and comply with applicable data protection law(s).*
>
> *27.3 ATAS shall implement reasonable cybersecurity measures (i.e. administrative, physical and technical safeguards) that are commensurate with accepted industry practices such as the ISO/IEC 27001:2013 – Information Security Management Systems – Requirements and the ISO-IEC 27002:2013 – Code of Practice for International Security Management."*

10. There have been credible reports since early 2018, including in the international press and trade journals, that Otan has been the target of cyberattacks from a mixture of private and state sanctioned actors involving both corporate and political espionage. SWF says that this constitutes relevant context to the data and cybersecurity provisions in the Agreement. Further, ATAS has refused to locate the servers for the Platform in Otan itself citing such cybersecurity concerns for that decision.

11. SWF has good reason to believe that the Platform's software and server (owned by and under the control of ATAS) have been compromised by a hacker group with links to a certain hostile state. In particular, SWF avers that technological backdoors were installed on the system which granted these hostile actors "superuser rights" i.e. they had system administrator rights which allowed them to make unrestricted system-wide changes.

12. In this regard, and pending disclosure and/or the administration of interrogatories (or any equivalent which the Tribunal may order), SWF relies on credible reports from Otan's intelligence service that the Platform's software and servers as well as the Participants' data have been compromised. Further, SWF has also come to learn that databases of the information of the Participants are being sold on the so-called DarkNet.

13. In the premises, SWF says that ATAS is in fundamental breach of the Agreement which SWF is entitled to terminate summarily pursuant to the express termination rights accorded to SWF thereunder and/or under the common law of Singapore. Further, pursuant to the terms of the Agreement, upon termination of the Agreement for fundamental breach, SWF is entitled to a copy of the Platform's source code and databases.

14. Notice of termination of the Agreement was therefore provided to ATAS on 16 August 2019 in accordance with the notice provisions in the Agreement.

15. However, ATAS disputes the validity of the termination and insists on continued performance of the Agreement by the parties. ATAS also refuses to provide SWF with a copy of the Platform's source code and databases in breach of the Agreement. As a result of this dispute, SWF issued a hold notice on 30 August 2019 to ATAS to immediately take steps to preserve all relevant documentation and other evidence relating to the dispute (both physical and electronic), including but not limited to the source code(s), databases and all log files in relation to the Platform.

16. The Agreement contains an arbitration agreement and a governing law clause, which provide respectively as follows:

> "***31. Dispute Resolution***
>
> *31.1 Any dispute, controversy or claim arising out of or relating to this agreement, or the breach, termination or validity thereof, shall be finally resolved by arbitration held in Singapore in accordance with the UNCITRAL Arbitration Rules for the time being in force.*
>
> *31.2 The Tribunal shall consist of three (3) arbitrators and the language of the arbitration shall be English. Each party shall appoint an arbitrator, and the two appointed arbitrators shall select a third arbitrator who shall be the presiding arbitrator of the arbitral tribunal.*
>
> *31.3 Either party to the arbitral proceedings commenced pursuant to this clause 31 may elect to conduct discovery pursuant to the US Federal Rules of Civil Procedure (save for depositions), subject always to the Tribunal's determination that such discovery is inappropriate in the circumstances and/or where such discovery would contravene any applicable mandatory norms or law.*
>
> ***32. Governing Law***
>
> *This Agreement shall be governed by and construed in accordance with the laws of Singapore.*"

17. In the premises, SWF requests the following relief in the form of a Final Award:
    a. A declaration that ATAS was in fundamental breach of the Agreement;
    b. A declaration that SWF was entitled to terminate the Agreement;
    c. An award of damages for breach of contract;
    d. An order that ATAS do provide a copy of the Platform's source code and databases to SWF;
    e. An award of interest on the damages and costs awarded at such rate and for such period as the Tribunal considers appropriate;
    f. An order that ATAS bear the legal and other costs of the arbitration, including the fees and expenses of the Tribunal; and
    g. Such further relief and other relief as the Tribunal considers appropriate.

Extracts from Statement of Defence

[…]

5. ATAS accepts that an intermediary had placed representatives from both SWF and ATAS in contact with one another. Pursuant to those initial contacts, parties entered into extensive negotiations before entering into the Agreement.

6. The development and successful launch of the Platform was meant as proof of concept and demonstrative of ATAS's capabilities to deliver on a product and services that were aligned with the Otanian 5 year programme. The intention was for SWF to invest substantially into ATAS if the beta-testing of the Platform proved to be viable. The ostensible funding pleaded by SWF was in actuality notional. The amount of the funding would not and indeed did not cover the substantial costs that ATAS incurred in the setting up of the Branch as well as the developmental work involved for the coding of the Platform.

7. As such, all intellectual property in the Platform would remain with ATAS. In this respect, ATAS highlights that the Platform contains, embeds and uses ATAS's proprietary software code and algorithms which promote health conscious behaviour in the Participants through the modification of their dietary, exercise and spending habits.

8. ATAS avers that continued ownership of the source code and its protection is of paramount importance to ATAS. This was because its intellectual property was what enables ATAS to differentiate itself from its competitors in the technology consultancy or software solutions business.

9. In fact, the parties agreed and it is a specific term of the Agreement that the parties' normal document retention and deletion policies would apply. SWF was aware that it was ATAS's corporate policy to only retain electronic information for a period of 12-months before the permanent and complete deletion of the same, including from any back-up servers.

[…]

15. In this respect, ATAS was well aware of the well-publicised reports of Otan being the subject of hostile and malicious cyber intrusions and was therefore concerns for the safety of its intellectual property rights as well as those of the Participants.

16. ATAS notes with concern the various news reports that Otan continues to be the target of sophisticated cyberattacks. In particular, it fears that the propagation of confidential information in the usual manner would render them vulnerable to attack across multiple attack vectors. In particular, each of parties' representatives, counsels in each law firm as well as Tribunal members are now potential targets for further malicious cyberattacks.

[…]

20. ATAS accepts that SWF was mindful to exclude citizens or residents of EU member states in the class of Participants on the Platform due to EU General Data Protection Regulation ("**GDPR**") concerns. However, parties nonetheless agreed that ATAS would establish up a branch in Otan and for purposes relating to the Platform. In this regard, the parties understood that the Branch would employ Otanians and citizens of other European member states as its employees doing software coding, marketing and other forms of data entry in relation to the Platform and any other new or existing projects which ATAS may assign to its employees.

21. Further, due to ATAS's operations in Otan through the Branch, it appointed a GDPR representative as well as a separate data protection officer, both of whom were based in Otan. However, since the commencement of the arbitration, both the GDPR representative and data protection officer have been uncontactable.
22. The Participants consented only to participate in the beta-testing of the Platform. They did not provide "freely given, specific, informed, unambiguous" consent for their data to be transferred to a third party country for purposes of any arbitration between the parties.

[…]

30. ATAS highlights that there are no audit rights or information rights in the Agreement and notes that SWF does not plead to the contrary.

[…]

35. ATAS denies that Platform, the relevant servers or the Participants' information were compromised. ATAS has its own in-house cybersecurity team who will attest to the same effect. Further, ATAS will rely on a Vulnerability Assessment and Penetration Test ("**VAPT**") Report produced by a reputable cybersecurity firm. The report will show that following a comprehensive VAPT there is no evidence of a hack and that there was nothing found in the audit logs which suggest malicious activity.

Procedural Background

1. On 2 September 2019, SWF served ATAS with a Notice of Arbitration pursuant to Article 3 of the UNCITRAL Arbitration Rules 2013 ("**UNCITRAL Rules**") referencing ATAS's wrongful breach of the Agreement. The Notice was served through SWF's appointed US counsel, Mary, Sue & Partners, a premier boutique disputes practice. In its Notice, SWF notified ATAS of the appointment of its co-arbitrator, Professor North Saw, an independent arbitrator and lawyer dual-qualified in the State of New York as well as England and Wales. He resides principally in London but has residences elsewhere in Europe.

2. On 30 September 2019, ATAS filed its Response to the Notice of Arbitration pursuant to Article 4 of the UNCITRAL Rules. The Response was served through ATAS's appointed counsel, Ang, Beh & Chan LLP, a leading Singaporean disputes firm. ATAS notified SWF of the appointment of its co-arbitrator, Ms. Regina Wang, S.C., a retired judge of Singapore's Court of Appeal.

3. On 7 October 2019, the two co-arbitrators appointed you, the presiding arbitrator, a tri-qualified lawyer residing principally in Singapore, from which date the arbitral tribunal ("**Tribunal**") was constituted. You are from the Singapore office of an international firm with offices across the US, Europe and Asia.

4. At the first procedural hearing, parties agreed first to file their pleadings and to defer issues regarding the extent of discovery/disclosure to the next procedural hearing, subject to any agreement that parties may subsequently reach on those issues.

5. Despite subsequent attempts, the parties were unable to come to an agreement on the appropriate directions and process for disclosure. This was complicated by ATAS's insistence on cybersecurity measures which it insisted were necessary for its compliance with the GDPR and its commercial interests. The parties therefore requested that the Tribunal deal with this and any ancillary issues at the second procedural hearing.

6. At the second procedural hearing by teleconference, the parties made extensive submissions on what processes should be adopted as regards discovery/disclosure and applicable cybersecurity measures. In summary:
   a. SWF mooted US style discovery as not being unreasonable and not otherwise in conflict with the GDPR (which SWF submits is inapplicable or otherwise of very limited relevance) or any other mandatory norm. SWF also considered that no special cybersecurity measures were necessary in the circumstances; and
   b. ATAS argued that it was subject to GDPR obligations and the GDPR applied to the conduct of the arbitration. The applicability of the GDPR placed restrictions on its disclosure of information, the extent to which it may validly comply with the Tribunal's orders and the necessary cybersecurity measures which it considered were necessary for its compliance with the same.

7. At the end of the teleconference, the Tribunal reserved its decision on what directions to order and the form in which such an order would take.

8. During the Tribunal's deliberations after the second procedural hearing, the co-arbitrators came to a consensus as to the most pertinent issues which they considered needed to be addressed in the Tribunal's orders/directions, even if they may have disagreed on the specifics of such an order.

Notes of Procedural Telephone Conference

Attendance

Tribunal

- Presiding arbitrator
- Professor North Saw
- Ms. Regina Wang, S.C.

Parties

- SWF, represented by Mary, Sue & Partners
- ATAS, represented by Ang, Beh & Chan LLP

Notes and Parties' submissions

1. During the first procedural hearing, both parties agreed that following the close of pleadings, the next issues to be resolved would involve discovery/disclosure of documents prior to the tendering of the respective parties' witness statements. In the course of the second procedural hearing, it became clear that both parties wanted a determination as to the appropriateness of US style discovery, the applicability of the GDPR to the arbitration proceedings as well as any applicable cybersecurity measures.

2. Parties also agreed that employee data, including sensitive personal data, would be made available through the disclosure process. It was agreed that these data would be covered by either the Singapore Personal Data Protection Act 2012 (the "**PDPA**") or the GDPR, and there was no dispute that the disclosure process would accordingly be governed by the provisions of the PDPA and/or GPDR (if applicable). However, the parties disputed the extent to which the GDPR would be applicable, if at all.

3. Parties also were unable to come to an agreement on the applicable cybersecurity measures to be applied to any disclosed information and in particular the Otanian intelligence report, the Platform's source code and copies of its database. Both parties referred to or otherwise relied on the Draft Cybersecurity Protocol for International Arbitration (Consultation Draft).

4. ***SWF's submissions***

   4.1. The Agreement is governed by Singapore law. The seat of the arbitration is Singapore. It follows that the implied choice of the governing law of the arbitration is also Singapore law.

   4.2. Notwithstanding the preceding, the parties had also agreed to apply US style discovery unless the Tribunal considered it to be unreasonable or it conflicted with a mandatory norm or provision of law. In this regard, the Tribunal ought to order a legal hold to prevent any destruction of documentations and evidence as may otherwise happen in the course of ATAS's business.

   4.3. GDPR does not apply as this is a contract between SWF, a Delaware corporation, and ATAS, a Singapore company. The (Singaporean) PDPA recognises the legal proceedings exception to the collection, use and

disclosure of personal data. Further, any issues regarding the transfer of personal information outside of Singapore can be dealt with by an appropriate protocol or direction under the PDPA.

4.4. SWF notes that were the GDPR to apply, then an order of the Tribunal would not suffice to compel specific disclosure of documents. The exemption of "*compliance with a legal obligation*" does not cover an order from the Tribunal as per Working Document 1/2009 on Pre-Trial Discovery for Cross Border Civil Litigation. SWF also refers to Article 48 of the GDPR and the corresponding recital. Further, the processing of sensitive personal data is also not subject to the exception of Article 49(1)(e) which is "*the transfer is necessary for the establishment, exercise or defence of legal claims*".

4.5. SWF also points out that the transparency requirement in the GDPR would render it mandatory to notify data subjects (e.g. the Participants) of the identity of any recipients, the purposes of the processing, the categories of data concerned and the existence of their rights (including a right to object to the processing of their data).

4.6. SWF is willing to provide redacted copies of the reports provided to it by Otan's intelligence service but subject to adequate cybersecurity measures to be ordered by the Tribunal and to SWF's satisfaction. In fact, SWF argues that for so long as it is provided with a copy of the Platform's source code and its database, there would be no need for it to adduce the intelligence report to demonstrate ATAS's breach of the Agreement.

4.7. In this regard, SWF says that anonymisation of or even pseudonymisation of the databases and personal information would be inappropriate as it would detract from the evidentiary value of proving ATAS's breach of the Agreement.

5. ***ATAS's submissions***

5.1. The real and closest connection under the Agreement is to Otanian law. The governing law of arbitration is therefore Otanian law.

5.2. US style discovery is unreasonable and contrary to the principles of the GDPR in any event. This includes any orders for a legal hold by the Tribunal. In this regard, ATAS notes Article 9.2(d) of the IBA Rules of the Taking of Evidence in International Arbitration which permits exclusion from evidence or production of a document on grounds of loss or destruction that has been shown with reasonable likelihood to have occurred.

5.3. In determining the applicability of the GDPR to this arbitration, the Tribunal should have regard to Guidelines 3/2018 on the territorial scope of the GDPR (Article 3). GDPR applies by virtue of the fact that ATAS has an establishment in Otan, a member-state of the European Union. Further, the server containing the database of Participants' information is located in Otan.

5.4. The Tribunal should also have regard to Working Document 1/2009 on pre-trial discovery for cross border civil litigation in terms of parties' compliance with the GDPR for: (a) retention; (b) disclosure; and (c) onward transfer. In this respect, ATAS notes that SWF is not Privacy Shield certified.

5.5. In accordance with the GDPR principle of data minimisation, ATAS proposes the use of an online file hosting service for centralised control of any and all documents submitted to the Tribunal and as

between the parties. ATAS says that apart from having an audit log of each file being accessed, there will be strict user control access to the uploaded files including but not limited to view-only rights as the default.

5.6. In particular, ATAS insists that its compliance with any disclosure orders made by the Tribunal (if applicable) must account for heightened cybersecurity measures for commercially critical intellectual property such as the source code for the Platform as well as the sensitive personal information in the database. ATAS submits that the centralised file hosting service can ensure that the source code can only be viewed but not downloaded and disseminated.

5.7. Since the GDPR applies to the arbitration, the Tribunal's order/protocol must have adequate data security, data minimization, transparent data retention policies, transparent processing information (potentially including data privacy notices), third country transfer restrictions, and data breach notifications.

5.8. ATAS was concerned by Professor North Saw's use of a popular free webmail account and raised issues as the extent to which such email accounts were secure.

6. Co-Arbitrators' consensus on issues raised and to be determined

6.1. Applicable seat of arbitration, governing law of arbitration and applicability of GDPR (and extent of which is applicable) to the arbitration.

6.2. The implications of US style discovery (if ordered). For example, should the Tribunal order "litigation holds" (i.e. preservation orders) even where it could detract from the parties' obligations under the GDPR (if applicable)?

6.3. The appropriate form of the Tribunal's orders, e.g. directions, orders or an agreement signed by all of the parties, bearing in mind procedural/logistical convenience and possible lack of cooperation by the relevant parties (including third parties) involved?

6.4. Other cybersecurity and data protection issues to be addressed include:

6.4.1. the transmission of communications, pleadings, disclosure materials and evidence by the parties;

6.4.2. communications among arbitrators and between the arbitrators;

6.4.3. storage of arbitration-related information;

6.4.4. sharing arbitration-related information with authorised third parties such as experts, interpreters, transcribers, and tribunal secretaries;

6.4.5. vulnerability monitoring and breach detection;

6.4.6. security breach notification and risk mitigation; and

6.4.7. post-arbitration document retention and destruction.

6.5. Whether procedural mechanisms such as a tribunal appointed expert will be an appropriate form of risk mitigation over technological approaches.

6.6. Professor North Saw notes that Otan, unlike the UK, has not opted out of Article 48 of the GDPR, which restricts an EU Member State from enforcing a judgment requiring the transfer or disclosure of personal data where there is no international agreement or treaty.

6.7. Professor North Saw says that his webmail account has 2-factor authentication, which should render it sufficiently secure against any malicious cyberattacks. Ms Regina Wang, SC, has her own private email server which is managed by a reputable IT firm. Both use multiple devices to access their electronics sent to them, including phones, tablets and laptops.

*