Debevoise & Plimpton

Protocol to Promote Cybersecurity in International Arbitration

Debevoise Protocol to Promote Cybersecurity in International Arbitration

As the prevalence of malicious cyberactors and cyberattacks on high-profile companies and government organizations grows, parties to commercially or politically sensitive international arbitrations increasingly express concerns with respect to cybersecurity. Cybersecurity threats may create significant operational and legal problems that can compromise the arbitral process, including loss or unauthorized disclosure of sensitive data, breaches of attorney-client confidentiality, adverse media coverage and reputational damage, costs associated with breach notification or data recovery, and legal liability. In addition to the threat cyberattacks pose to the parties to an arbitration, failing to address this problem could ultimately lead to a loss of confidence in the arbitral system.

To respond to these concerns, the practitioners at Debevoise & Plimpton LLP have developed this Protocol to Promote Cybersecurity in International Arbitration. This Protocol operates on three principles: (i) Establishing Secure Protocols for the Transfer of Sensitive Information at the Outset of Proceedings, (ii) Limiting Disclosure and Use of Sensitive Information, and (iii) Developing Procedures for Disclosing Cyber Incidents.

The Protocol reflects our continued commitment to counsel clients on the most critical issues in international arbitration. We believe consideration of the procedures reflected in this Protocol will improve the arbitration process while appropriately managing risks. The procedures reflected in this Protocol are meant to be adaptable, so that parties, counsel and arbitral tribunals can use the flexibility inherent in international arbitration to develop procedures relevant and appropriate for each individual arbitration.

Protocols for Transfer and Storage of Sensitive Information

1. We will request that the arbitral tribunal establish protocols and procedures for the transfer of sensitive information at the outset of proceedings, usually in the first procedural conference. What constitutes such sensitive information should be defined in light of the particular circumstances of a dispute.
    a. These protocols and procedures may include: (i) defining categories of sensitive information, updated as necessary through the course of the proceeding; and (ii) agreeing on processes for the secure transfer of such sensitive information between and among the tribunal and the parties.
    b. This may include barring certain transfer methods (e.g., use of public WiFi to access sensitive information) or adopting certain transfer methods (e.g., use of secure portals instead of email).
2. We will ask the arbitral tribunal and the parties to consider and, if appropriate, agree to specific encryption standards for the transmission of sensitive information.
3. We will propose and encourage arbitral tribunals to disfavor the use of insecure email for the transmission of sensitive information unless additional measures are taken to secure the information. Such additional measures may include applying passwords to documents containing sensitive information that will be transmitted via separate channels (e.g., texting or via a phone call).
4. We will propose that, where possible, email accounts maintained by third party public servers (e.g., Gmail) have additional access protections such as multi-factor authentication (e.g., use of a token or similar mechanism in addition to username and password).
5. If third-party cloud storage is used, we will consider whether the third-party cloud storage incorporates adequate security protocols.
6. We will consider, and ask that the arbitral tribunal and opposing party consider, applicable governmental cross-border restrictions on the transfer of sensitive information and adopt reasonable measures to facilitate compliance with any restrictions.

Limited Disclosure and Use of Sensitive Information

7. Before submitting any sensitive information to the arbitral tribunal or opposing party, we will weigh the sensitivity of that information against the relevance and materiality of that information for that arbitration.
8. We will explore with the arbitral tribunal whether sensitive information may be submitted in a form that is only screen viewable (i.e., not downloadable or printable). If sensitive information is permitted to be printed, we will ask the tribunal to establish consistent policies and procedures related to the destruction of printed materials.
9. To the extent practicable, we will limit the persons who have access to sensitive information to those persons having a need-to-know with respect to such information.
10. To the extent practicable, access to sensitive information on computer systems should be restricted to those using a secure log-in ID and password, with a unique log-in ID and password assigned to each individual. We will consider, and ask that the arbitral tribunal and opposing party consider, the use of multi-factor authentication to access accounts or portals used to transmit and receive sensitive information.
11. We will restrict the ability to transfer sensitive information to mobile devices only if they use encryption or other appropriate security protocols.
12. At the client's request, we will establish procedures for returning or destroying sensitive information upon the conclusion of the arbitration.

Procedure for Disclosing Data Breaches

13. We will take reasonable steps to mitigate any potential breach, including by contracting with third-party vendors as necessary.

14. We will propose and work with the arbitral tribunal to establish policies and procedures related to detecting breaches, determining their scope, and notifying affected parties. Where the existence of the arbitration is itself confidential, we will work with the tribunal to consider means of notifying affected parties that best preserve the confidentiality of the arbitration.

15. We will propose and work with the arbitral tribunal to establish point-persons for each party to the arbitration and the tribunal itself to be responsible for coordinating communications in the event of a data breach or other incident that exposes or affects sensitive information.

16. We will consider whether there are any legal obligations to report the breach to affected parties, regulatory agencies, or other authorities.

Debevoise & Plimpton

New York
919 Third Avenue
New York, NY 10022
+1 212 909 6000

Washington, D.C.
801 Pennsylvania Avenue N.W.
Washington, D.C. 20004
+1 202 383 8000

London
65 Gresham Street
London
EC2V 7NQ
+44 20 7786 9000

Paris
4 place de l'Opéra
75002 Paris
+33 1 40 73 12 12

Frankfurt
Taunustor 1 (TaunusTurm)
60310 Frankfurt am Main
+49 69 2097 5000

Moscow
Business Center Mokhovaya
Ulitsa Vozdvizhenka, 4/7
Stroyeniye 2
Moscow, 125009
+7 495 956 3858

Hong Kong
21/F AIA Central
1 Connaught Road Central
Hong Kong
+852 2160 9800

Shanghai
13/F, Tower 1
Jing'an Kerry Centre
1515 Nanjing Road West
Shanghai 200040
+86 21 5047 1800

Tokyo
Shin Marunouchi Bldg. 11F
1-5-1 Marunouchi, Chiyoda-ku
Tokyo 100-6511
+81 3 4570 6680

www.debevoise.com