The 2018 Update to the CPR’s Non-Administered Arbitration Rules: A Reflection of Current Trends in Arbitration

CLIENT ALERT | April 20, 2018

Albert Bates Jr. | batesa@pepperlaw.com
R. Zachary Torres-Fowler | torresr@pepperlaw.com

This article was published in the April 2018 issue of ConsensusDocs (Vol. 4, Issue 2). It is reprinted here with permission.

On March 5, 2018, the International Institute for Conflict Prevention & Resolution (CPR) unveiled its revised Non-Administered Arbitration Rules (the CPR Non-Administered Rules). The 2018 revisions mark the first update to the CPR Non-Administered Rules since 2007 and generally reflect ongoing trends in arbitral practice.

Although the CPR began offering administered arbitration services in 2013, the CPR is best known for its Non-Administered Rules for ad hoc domestic business-to-business arbitration. The 2018 revisions to the CPR Non-Administered Rules include, among
others, provisions concerning multiparty arbitration, the apportionment of costs, and emergency arbitration—features that are relatively common among leading arbitration rules.¹

There are, however, a pair of revisions that are worth a second look: the “screened selection” process and cybersecurity measures. While the CPR’s “screened selection” process and cybersecurity measures are not entirely new to the arbitration community, they reflect efforts by arbitral institutions to address concerns with the dispute resolution process. As a result, arbitration users within the construction industry are well advised to familiarize themselves with these trends.

**Screened Selection Rule**

In its inaugural Administered Arbitration Rules from 2013, the CPR incorporated a “screened selection” process for party-appointed arbitrators. At its core, the CPR’s screened selection process enables the parties to select party-appointed arbitrators without informing the arbitrator-candidates of the appointing party in order to eliminate perceived bias by party-appointed arbitrators to their appointing party.²

The 2018 revisions allow parties to select the CPR’s screened selection procedures in the CPR Non-Administered Rules. According to Rule 5.4, if the parties have opted into the CPR’s screened selection process, the CPR will invite the parties to provide a list of potential arbitrators to the CPR, drawn in whole or in part from the CPR’s Panels of Neutrals, to be circulated between the parties by the CPR. At the time the CPR circulates the parties’ list of potential candidates, the CPR also provides a confirmation of the candidates’ availability and the disclosure of any circumstances that might give rise to concerns over the candidates’ lack of impartiality or independence. From the list of candidates, the parties select three candidates, in order of preference, for their party-appointed arbitrator and notify the CPR and opposing party of their selections in writing. If there are no objections to the most preferred candidate on either parties’ list, then each party’s first choice is appointed by the CPR. If a party reasonably objects to the opposing party’s first choice, the CPR then moves down the list of potential arbitrators until an unobjectionable candidate is selected. Importantly, throughout this process, the CPR ensures that the potential party-appointed arbitrators remain unaware of the party that selected them.

While other institutions have utilized similar procedures, the CPR’s 2018 revisions suggest that “blind” or screened selection procedures are gaining greater acceptance in the marketplace.³
CPR’s Cybersecurity Measures

The 2018 update to the CPR Non-Administered Rules also includes a new provision concerning data protection and cybersecurity measures. With reference to the initial pre-hearing conference, Rule 9.3(f) provides that the parties may consider a variety of matters concerning the administration of the arbitration, including “[t]he possibility of implementing steps to address issues of cybersecurity and to protect the security of information in the arbitration.” By including an explicit reference to cybersecurity, the 2018 revisions suggest that tribunals consider adequate measures to ensure the protection of the parties’ confidential information.

The CPR’s efforts to focus attention on cybersecurity in arbitration are commendable, as the need to protect confidential information is among the most pressing issues facing the legal community and its clients. Rule 9.3(f) takes a significant step forward from prior rules by explicitly reminding all tribunals to discuss data protection and cybersecurity issues at the outset of the arbitration.

The arbitral institutions, including the AAA, ICC, CPR, and others, have made significant investments in recent years toward securing their IT systems, and the data provided to them, during the course of an arbitration. Law firms and their clients have similarly made significant investments in cybersecurity and data protection. The weakest link tends to be the arbitrators, many of whom are sole practitioners who lack the technical support provided by larger organizations and many of whom may not have “grown up” with a computer on their desk. Certainly, arbitrators are mindful of their duty to protect the confidentiality of the arbitration information, and they secure their arbitration papers in their office or home office. However, they may not always fully consider the policies needed to secure the electronic data of the parties to the arbitration. The days of boxes of binders and paper have been replaced with thumb drives, hard drives, cloud storage, and secure drop boxes. Data may be downloaded or viewed in hotels or coffee shops or on other public or non-secured networks. Some or all of the data may accessible on the arbitrator’s personal desktop, laptop, tablet, phone, thumb drive, hard drive and/or other portable devices. In short, the security of this arbitration data rests with the arbitrator who possesses or has access to it, and that protection may only go as far as the arbitrator’s own technological savvy.

The CPR should be commended for reminding arbitrators to discuss issues of cybersecurity and data protection at the initial pre-hearing conference. Rule 9.3(f) facilitates the discussion between the tribunal and the parties from the outset of the case and, as best practices would suggest, may ultimately produce an appropriate confidentiality and data protection protocol for each case.
Conclusion
While the CPR’s 2018 revisions generally reflect features that are relatively common among leading arbitration rules, they are an indication of where future arbitral practice is headed. As a result, construction industry leaders should be mindful of these developments in alternative dispute resolution.

Endnotes


3. While the AAA has informally offered list and appointment services on non-administered matters for a long time, it formally began offering the AAA’s “À La Carte Services” for non-administered cases, including similar assistance with the screening, selection and “blind” appointment of arbitrators, in 2016.

4. It has been reported that the Permanent Court of Arbitration at the Hague was hacked in 2016 during the course of a contentious and widely reported arbitration it administered between the Philippines and China involving historic rights and maritime entitlements in the South China Sea. This event has contributed to the speed with which arbitral institutions have addressed their cybersecurity issues.

5. Additional training for arbitrators and their staff in data protection and cybersecurity has been the subject of discussion at many arbitral institutions. For example, the AAA recently announced a cybersecurity training initiative for arbitrators. It is likely that other providers will also make data protection and cybersecurity training a priority for arbitrators.