Appendix E - Checklist of Issues to Consider When Choosing an Online Case Management Platform

Definitions	For the purpose of this checklist, the following terms are defined as follows: > 'OCMP': online case management platform > 'Users': parties, arbitral tribunals, administrative secretaries, the institution and, as the case may be, experts > 'Communications': e-mails, messages, correspondence, any type of document (submissions, exhibits, witness statements, expert reports, procedural orders, decisions, awards) > 'OCR': optical character recognition > 'DRO': dispute resolution organisation
Core service to be provided by an OCMP	The cornerstone to successfully motivate the Users to make use of an OCMP is its capability to standardise and centralise information, and to make that information easily accessible. An OCMP secure system should offer the possibility to generate, send, receive, store, retrieve, exchange or otherwise process Communications (including, but not limited to, large sensitive documents) used in an arbitration, as well as tracing of the Communications.
Other services offered by an OCMP	The platform should initially present general information to any visitor and user: > Video or other tutorial of the platform's basic functions and features. > News informing about any upgrades and additional services offered. > Whether technical support is available 24/7. > Whether there is a default folder structure available and the nature thereof. > The OCMP's level of security in all aspects and whether the platform benefits from a security certifying body (i.e. ISO standard) and displays the certificate logo of such certifying body. > The applicable data protection regulation (i.e. governing jurisdiction) and geographical location of primary storage of data and backup storage (where servers and/or encryption keys are located). > Whether the transfer of any data and document is end-to-end encrypted during transfer and whether stored data is encrypted. > Service and maintenance of the OCMP without access to readable content. > Whether the service employs zero-knowledge encryption: (i) who has access to the encryption keys (the DRO and/or third-party OCMP supplier or possibly a DRO; and (ii) can the encryption keys be deposited with a third party in another jurisdiction (to protect the parties against court orders generated by third parties or authorities outside the ongoing arbitration case). .../...

CONTENTS

Other services offered by an OCMP (continued)	> Format of materials which may be uploaded (for example, .docx, .xsls, .pdf, .jpeg, .mov, .mp4) and whether it takes compressed files, locked PDFs etc. (the arbitral tribunal may wish to request both locked and searchable versions of documents in a procedural order). > Maximum size accepted for each material. > Languages recognised by the OCR. > Whether keyword search and filtering is possible. > Whether the OCMP has an integrated hearing facility, including break-out rooms, recording, etc. (see checklist on virtual hearings) and whether it offers any troubleshooting assistance during hearings. > Whether Users can create their own individual space within the case to prepare material for a hearing and for personal notes to be saved in such space, with mark-up tools. > The provider's procedure for entering into the contract and which participant(s) to the arbitration will be signatories to the contract with the OCMP provider. > Information on the login techniques for registered individuals.
Terms and conditions of service	The OCMP's terms and conditions may be non-negotiable but must be acceptable to all Users of the platform. The OCMP should undertake to take reasonable steps to remedy any interruption of the system as quickly as possible, if such interruption is on its/their system. However, the following exclusions of liability are typical: exclusion of liability for the content of Communications uploaded by the Users on the platform; exclusion of liability for any internet interruption, speed, performance or otherwise, which cannot be guaranteed, or for any problem of connection or any other technical problem unrelated to the services offered by the OCMP. Terms and conditions should indicate the default period during which parties and the arbitral tribunal may still access their case on the OCMP at the end of the arbitration. However, the parties and the arbitral tribunal may agree on a shorter or longer period (see 'Document retention' below).
Agreement and Commitment to use the OCMP for the arbitration	Commitment to use the OCMP should be recorded in an agreement by the parties and/or a procedural order that addresses the following. Scope of use: parties and the arbitral tribunal should decide if they wish to use the service for complete management of the case online (e.g. built-in secure videoconferencing, e-bundling of documents), or if they wish to use it only as a repository, i.e. for upload, download and storage of Communications. Document retention: The parties and the arbitral tribunal may agree on a shorter or longer period than the default retention period for data by the OCMP. At the end of the period during which access to the case is possible, the OCMP may destroy any data and documents uploaded. Other procedural agreements: consider procedural aspects such as who will bear the costs, exclusions of liability, or rules concerning access rights and security. Default rules for organising documents and uploading files: naming conventions for folders and files must be standardised for the OCMP to be of maximum benefit. (See below for sample structure.)

CONTENTS

Acceptance by the DRO, if applicable	If there is an administering institution, it should agree that use of the OCMP is acceptable to it.
Equipment	Users should ensure they have the necessary equipment enabling them to access the OCMP, including but not limited to suitable software, hardware and internet connection.
Access credentials	Users should keep their access credentials strictly confidential.
Confidentiality and authorised Users	Access to the case on the OCMP should be limited to the parties and/or their representatives, the arbitral tribunal, any administrative secretary, and the DRO. A list of such Users must be established and shared with the Users or simply listed in the OCMP. (See below, organisation of sections of the OCMP.)
Uploading of documents	Parties and the arbitral tribunal should commit to upload on the OCMP any Communication, unless otherwise agreed by the parties and the arbitral tribunal where Communications would preferably be transmitted in hard copy due to their size or legibility (e.g. construction plans or large spreadsheets). Once uploaded on the OCMP, no Communication should be deleted, recalled or amended in any way (similarly to sending documents by post).
Alerts following upload	The OCMP should send automatic alerts to the Users in an arbitration for every Communication uploaded by any User. Such alerts should be sent to the intended recipients of the Communication. The arbitral tribunal and the parties should discuss the issue of proof of opening a message and downloading of a document being provided to the sender of the Communication (e.g. proof of downloading procedural directions by the parties *vs.* proof of downloading the parties' exhibits by the arbitral tribunal). In addition to indicating the e-mail address they wish to use in the arbitration, Users must ensure that the e-mail address sending alerts is whitelisted and does not land in a spam-box. Users should also regularly check the OCMP to make sure they have not missed a communication and to verify the various procedural dates.
Authors of uploading	Documents should be uploaded directly by their authors. The OCMP does not upload documents on behalf of a party or the arbitral tribunal. Tracing the author of an uploading, the date and time such uploading took place is important and must be ensured by the OCMP.
Default rules for organisation of case information, folders and uploaded documents	Consideration should be given to organisation of the following, which may be done by default by the OCMP or subject to customisation by the Users. Overview of the case: names of parties, their representatives and arbitrators, as well as administrative secretary, global amount in dispute, place of arbitration, applicable law, language of arbitration, stage of the procedure. Contact details of all Users in a case. Arbitral tribunal: names, who appointed them, date of their appointment, access to their CV and statement of independence, including comparable data for the administrative secretary. ... /...

CONTENTS

Default rules for organisation of case information, folders and uploaded documents (continued)	Financial aspect of the case, including amounts in dispute, payments of the advance made by the parties, expenses incurred by the arbitral tribunal, fees of the arbitral tribunal and any administrative secretary. Timetable: all deadlines fixed in a procedure, any extension granted and if the expected performance was met. Correspondence: all correspondence uploaded by any User. Submissions: upload should only be made available to parties. Exhibits: upload should only be made available to parties. Procedural orders: upload should only be made available to the arbitral tribunal, and any administrative secretary. Terms of reference and awards: upload should only be made available to the arbitral tribunal, any administrative secretary. Index of all documents: all documents uploaded on the platform in a chronological order. Common bundle: if parties produce a common bundle for a hearing. Forums: as follows to allow defined separate groups of Users to communicate amongst themselves (with the exclusion of other Users) without leaving their secure arbitration environment and avoiding any mistaken recipient. Sorting order: all sections with documents, financial aspect and timetable should offer the possibility of sorting information and documents in various orders, such as newest to older date and vice-versa, only documents posted by a given author, only types of documents uploaded (example submissions), only formats of document (for example, .pdf). Referencing of documents: when uploading Communications, the system should allow dropdown menus of standard information to be selected for uploading documents: > date format: yyyy-mm-dd for year-month-day > case reference used by a DRO or proposed by an OCMP > an abbreviation for each type of User (e.g. 'C' for claimant) > an abbreviation for document type (e.g. 'L' for letter; 'Ex.' for exhibit; 'WS' for witness statement; 'ER' for expert report) > brief further description (e.g. 2021-10-10 ICC 12345 C L time to cross-examine witnesses; 2021-09-17 ICC 23456 R Reply on Jurisdiction)

CONTENTS