

CHECKLISTE INFORMATIONS- UND KOMMUNIKATIONSTECHNOLOGIE & SCHIEDSVERFAHREN

(für Schiedsgericht & Parteien)*

A. Klärungsbedürftige Vorfagen

- Möglichst frühe Klärung der Geheimhaltungs- und Sicherheitsanforderungen im konkreten Verfahren als Grundlage für die Auswahl der Informations- und Kommunikationstechnik (IKT) für das Verfahren, insbesondere Bedrohungs-/Risikoanalyse, technische Fähigkeiten der Parteien, technische Kooperationsbereitschaft aller Beteiligten.
- Abwägung, ob sich die in Betracht kommenden IKT-Lösungen widerspruchsfrei in die DIS-Schiedsgerichtsordnung und die zwingende *lex arbitri* einbetten lassen; sowie ob keine Partei mit unangemessenem, ungerechtfertigtem Aufwand belastet oder benachteiligt wird.

B. Bei Verfahrensbeginn: Einsatz von IKT für Schreiben, Schriftsätze und Anlagen:

1. In welchem Umfang wird IKT für den Schriftverkehr genutzt werden?

- Schriftverkehr ausschließlich im elektronischen Format (Verzicht auf Papier, soweit nach DIS-Schiedsgerichtsordnung und anwendbarem zwingendem Recht zulässig)?
- Nur zur fristwahrenden Vorabübermittlung mit anschließendem Versand gedruckter Originale im Parteibetrieb?
- Unterschiedliche Regelungen für bestimmte Kategorien von Dokumenten?

2. Welche Datenformate und -bezeichnungen werden genutzt?

- Dateiformate, Durchsuchbarkeit mittels Texterkennung (OCR)?
- Einheitliche Dateibezeichnungen d.h. („sprechende“ Dateinamen, die zur Bezeichnung im Schriftsatz korrelieren)?

3. Wie werden Schreiben, Schriftsätze und Anlagen übermittelt?

- Per Email:
 - Verschlüsselt / unverschlüsselt (ggf. Verschlüsselungsmethode)?
 - Im Email-Anhang, z.B. als komprimiertes, passwortgeschütztes Dateiarchiv (ggf. Verschlüsselungsstandard, Passwortaustausch)?
 - Zu berücksichtigende andere technische Einflussfaktoren (Volumenbegrenzungen, Spamfilter, etc.)?

* Diese Checkliste wurde von einer aus dem Kreis des DIS-Beirates heraus arbeitenden, von Viktor von Essen gegründeten Arbeitsgruppe zu Anlage 3 lit. G zu Art. 27.4 2018 DIS-Schiedsgerichtsordnung verfasst. Die DIS dankt den Mitgliedern dieser Arbeitsgruppe, die nachfolgend aufgelistet sind: *Silke Elrifai, Dr. Richard Happ, Dr. Sebastian D. Müller, Karl Pörnbacher, Dr. David Quinke, Tamay Schimang, Erik Schäfer, Dr. Joseph Schwartz, Dr. Anke Sessler, Prof. Dr. Rolf Trittmann*. Die DIS ist für Änderungs- und Ergänzungsvorschläge dankbar. Bitte übersenden Sie diese per E-Mail an casemanagement@disarb.org und tragen Sie in der Betreffzeile den Begriff „Datenschutz“ ein.

- Regeln zu Fristwahrung, Eingangsbestätigung?
- Per sFTP-Server:
 - Welcher Server, wie gesichert, Passwortaustausch, Format der hochzuladenden Dateien (z.B. passwortgeschütztes Dateiarhiv oder einzelne, ungepackte Dateien)?
 - Regeln zu Fristwahrung, Pflicht zum Herunterladen, Eingangsbestätigung, etc.?
- Per Datenraum in der Cloud:
 - Welcher Datenraum (-Provider), wer organisiert, wie werden die Bereiche (Verzeichnisse) und Zugriffsberechtigungen (Lese-, Schreib-, Löschrchte) organisiert?
 - Regeln zu Fristwahrung, Pflicht zum Herunterladen/zur Kenntnisnahme, etc.?
- Per körperlich übermitteltem Datenträger:
 - Festlegung des Datenträgers (z.B. Flash Memory (USB), CD, DVD, Blu-ray, portable Festplatte)?
 - Klärung technischer Beschränkungen, z.B. unzulässige und technisch verhinderte Anschlussmöglichkeit von USB-Medien im Empfängersystem, Lese- bzw. Schreibmöglichkeit von optischen Medien;
- Für alle Varianten: Regelungen zu Störungen, Benachrichtigungspflichten, Folgen von Versäumnis?

C. Einsatz von Videokonferenzen

- Bei Verfahrensbeginn oder später zur Vorbereitung der mündlichen Verhandlung: Klärung, ob und für welche Teile des mündlichen Verfahrens Videokonferenzschaltungen effizienzsteigernd eingesetzt werden, also für:
 - Besprechungstermine zwischen Schiedsgericht und Parteien zur Verfahrenssteuerung;
 - Zeugen und Sachverständigenbefragung;
 - die Verhandlung (insbesondere im Eilverfahren und bei kurzer Dauer, geringer Komplexität oder geringer Bedeutung des Streitfalls) oder
 - interne Beratungen des Schiedsgerichts ohne Beteiligung der Parteien?
- Welcher Videokonferenzprovider, wer organisiert, welche technischen Voraussetzungen (z.B. Ausstattung an den Zugriffspunkten, Möglichkeiten zur Anzeige von Dokumenten), Test erforderlich?

D. Technik in der mündlichen Verhandlung

- Anlässlich der Vorbereitung der mündlichen Verhandlung:
 - Klärung, ob Einsatz technischer Mittel (z.B. Vorhalt von digitalen Kopien historischer Unterlagen, Präsentationen, Videosequenzen, Simulations-, Berechnungsprogrammen, Grafiken) im Rahmen des Parteivorbringens, für Sachverständigen- sowie Zeugenbefragungen beabsichtigt ist;
 - Klärung der technischen Voraussetzungen (Netzwerkverbindung, Anzeigegeräte, usw.) und Verantwortlichkeiten für die Schaffung derselben;

- Einsatz technischer Mittel zur Aufzeichnung der mündlichen Verhandlung: Ton-/Videomitschnitt, Echtzeit-Transkription (technische Voraussetzungen und Verantwortlichkeit dafür, Kosteneffizienz) nachfolgende Transkription des Tonmitschnitts oder traditionelle Protokollierung der Verhandlung?
- Abwägung, ob Einsatz technischer Mittel effizienzsteigernd und angemessen (siehe lit. A, 2. Punkt);
- Bei der Nutzung von Videokonferenzdiensten (oben lit. C) in der Verhandlung: Vorkehrungen zur Vermeidung von Beeinflussungen der Zeugen/Sachverständigen (z.B. Anwesenheit von Entsandten vor Ort), Regelungen für Vorhalten von Unterlagen.

E. Sicherheit und Datenschutz

1. Sicherheitsmaßstab: Bedrohungsbewertung nach lit. A.

2. Datenschutzmaßstab: Gesetzliche Verpflichtungen:

- Pflichten der Beteiligten zur Sicherung der technischen Funktionen und Systemintegrität; z.B. höchstpersönliche Passwortverwaltung, Zugriffssicherheit bei den Parteien und Schiedsrichtern; Benachrichtigungspflichten bei vermuteten Intrusionen; Kooperationsverpflichtungen bei Vorfällen;
- Welche Maßnahmen sind notwendig oder nützlich, um Schiedsrichtern und weiteren Verfahrensbeteiligten die Einhaltung ihrer etwaigen Pflichten im Rahmen des Schutzes von personenbezogenen Daten zu ermöglichen bzw. zu erleichtern?

Rahmenbedingungen für alle oben angesprochenen IKT Dienste: Klärung und Berücksichtigung der Sicherheits- und Datenschutzerfordernungen für die gewählten Lösungen (Ort der Datenspeicherung bei Cloud-Diensten oder Beteiligten außerhalb der EU, Geschäftsbedingungen der Dienste, Zugriffsrechte auf Providerseite, etc.).