

Von Erik Schäfer, Düsseldorf*

Informationstechnologie in Schiedsverfahren nach 2018 DIS-Schiedsgerichtsordnung – Hinweise zu Art. 27.4(i) und Anlage 3 lit. G 2018 DIS-Schiedsgerichtsordnung

Vorbemerkung:

Der nachfolgende Leitfaden ist als eine Art „Beiprodukt“ anlässlich der Arbeiten einer aus dem Kreis des DIS-Beirats heraus arbeitenden Arbeitsgruppe zu Anlage 3 lit. G zu Art. 27.4 2018 DIS-Schiedsgerichtsordnung entstanden, der *Silke Elrifai, Viktor von Essen, Dr. Richard Happ, Dr. Sebastian D. Müller, Karl Pörnbacher, Dr. David Quinke, Tamay Schimang, Dr. Joseph Schwartz, Dr. Anke Sessler, Prof. Dr. Rolf Trittman* und der Verfasser angehören. Für wichtige inhaltliche Kommentare und Beiträgen zu danken ist auch *Harald Eul, Philipp Schauman, Frederik Leenen* und *Sebastian Feiler* mit ihrer Expertise in den Bereichen Datenschutz, Datensicherheit, Informations- und Datenverarbeitungstechnik.

Dem Leitfaden liegt die Aufgabe zugrunde, einen Überblick über die heute verfügbaren, ohne größeren Aufwand zugänglichen Mittel zu geben, welche helfen, die sichere digitale Kommunikation und den Umgang mit digitalisierten Aktenbestandteilen in Schiedsverfahren erleichtern. Der Verfasser arbeitet seit ca. 1986 mit einem eigenen PC und hat eine Arbeitsgruppe der ICC-Kommission für internationale Schiedsgerichtsbarkeit als *Co-Chair* geleitet, die im Abstand von fast 10 Jahren zwei Berichte vorgelegt hat. Die dabei gewonnenen Einblicke und die gehörten *war stories* haben ihn zu dem Schluss geführt, dass zwar Begriffe wie „neue Technologien“, „Blockchain“ oder „AI“ leicht in aller Munde geführt werden, dabei aber die Nähe zur praktischen Nutzung, die Kenntnis von der Leistungsfähigkeit und Handhabung der existierenden Werkzeuge irgendwie fehlt. Augenscheinlich wird im Durchschnitt in Schiedsverfahren das schon länger existierende Werkzeugpotenzial nicht voll ausgeschöpft – vermutlich weil zu viel Abstimmungsbedarf und Störpotenzial für das einzelne Verfahren befürchtet wird. Wenn alle Verfahrensbeteiligten über Werkzeugkenntnis verfügten, würden sich diese Befürchtungen leicht als unbegründet herausstellen. Deshalb versucht der Leitfaden, die angenommene Lücke zwischen abstraktem Wissen und konkreter Kenntnis der Werkzeuge so weit wie möglich zu schließen. Allerdings kann er nicht die Anwendungsnähe zum Werkzeug herstellen, die ein Nutzerhandbuch oder das Lernen durch Probieren bietet. Ein Schritt, um der Technologieentwicklung nicht nach sondern mit ihr mit zu laufen, sollte so getan werden können.

Der Leitfaden ist nicht der Weisheit letzter Schluss. Denn gerade in einem dynamischen technischen Umfeld gibt es stets Raum für Verbesserungen. Auch im Hinblick auf zukünftige Aktualisierungen des Textes freuen sich die DIS (Viktor.vonEssen@disarb.org) und der Verfasser (eschaefer@cohausz-florack.de) auf Kritik und Anregungen aus dem Leserkreis.

* *Erik Schäfer* ist Rechtsanwalt und Partner der Kanzlei COHAUSZ & FLORACK Patent- und Rechtsanwälte Partnerschaftsgesellschaft mbB in Düsseldorf. Dieser Leitfaden ist auch in der SchiedsVZ erschienen (*Erik Schäfer, SchiedsVZ 4/2019, S. 195 ff.*).

I. Kurerläuterungen zu Art. 27.4(i), Anlage 3 lit. G 2018 2018 DIS-Schiedsgerichtsordnung

1. Zweck

Diese Erläuterungen sollen den Verfahrensbeteiligten Anregungen an die Hand geben, um über den Wortlaut der Art. 4.1, 4.2, 27.4 2018 DIS-Schiedsgerichtsordnung hinaus die Effizienz von Schiedsverfahren mit Hilfe der Nutzung heute verfügbarer technischer Mittel zu steigern. Ob die aufgezeigten Mittel für den Einzelfall geeignet sind, muss der Leser selbst prüfen und entscheiden.¹ Die Umsetzung wird regelmäßig Unterstützung durch technisch qualifizierte Fachleute erfordern.

2. Verfahrensmanagement, Zeitplan

Der Einsatz technischer Lösungen für den Schriftsataustausch und die Kommunikationssicherheit ist frühestmöglich nach Bildung des Schiedsgerichts abzustimmen, damit alle Verfahrensbeteiligten dadurch die Effizienz steigern können. Die Verfahrensmanagementkonferenz (Art. 27.2 2018 DIS-Schiedsgerichtsordnung) ist der übliche aber auch letzte Zeitpunkt hierfür, auch wenn dieser Punkt getrennt, zB telefonisch bzw. schriftlich, abgehandelt werden kann.

Einzelheiten des Einsatzes von technischen Lösungen in der mündlichen Verhandlung können zu diesem Zeitpunkt noch nicht absehbar sein. Sie müssen dann rechtzeitig vor dem Termin in einer weiteren Verfahrensmanagementkonferenz geklärt werden, damit ausreichend Vorbereitungszeit zur Verfügung steht.

3. Anordnungen des Schiedsgerichts und Vereinbarungen

Die Erfahrung zeigt, dass der Einsatz technischer Lösungen die Kooperation aller Beteiligten einschließlich der Schiedsrichter erfordert, wenn es zu keinen absehbaren Störungen kommen soll. Deshalb sind im Regelfall nicht abgestimmte Anordnungen zu ICT²-Aspekten nicht vorteilhaft (siehe hierzu unten II.10.c).

Gleichzeitig können sich abgestimmte technische Abläufe erfahrungsgemäß unvorhergesehen komplizieren. Deshalb ist es wichtig, dass Regelungen zu technischen Kommunikationsabläufen und anderen ICT-Aspekten im Schiedsverfahren nicht als Parteivereinbarung, sondern verfahrensleitende Anordnung mit Änderungsvorbehalt für das Schiedsgericht auf dessen eigene Initiative oder Parteienantrag erfolgen. Jedoch wird regelmäßig vor der Änderung eine Abstimmung mit den betroffenen Verfahrensbeteiligten erfolgen.

¹ Diese Handreichungen für den Einsatz der Kommunikations- und Informationstechnologie in DIS-Schiedsverfahren dienen ausschließlich dem Zweck, den allgemeinen Kenntnisstand über deren effizienteren Einsatzmöglichkeiten zu heben und beanspruchen nicht, für jeden Einzelfall geeignet oder in allen Einzelheiten fehlerlos zu sein. Sie berücksichtigen die Verfahren vor staatlichen Gerichten nicht, die das Schiedsverfahren oder die Anerkennung, Aufhebung sowie Vollstreckung von Schiedssprüchen betreffen. Auch die „elektronische Schiedsakte“ ist deshalb so zu führen, dass mögliche Verfahren vor staatlichen Gerichten gemäß deren Form- und Kommunikationsvorschriften geführt werden können. Soweit konkrete technische Produkte erwähnt werden, dient dies der Illustration und als Aufforderung zur eigenen weiteren Recherche; ist also nicht als Vorgabe oder Empfehlung zu verstehen. Mehr können derartige Handreichungen nicht leisten. Schiedsrichter und Parteien müssen deshalb, möglichst unter Beiziehung von technischem Fachpersonal, die technischen Lösungen und Vorgehensweisen eigenverantwortlich festlegen, die gewünscht sind und die möglichst unkompliziert für ihre Bedürfnisse funktionieren sollen. Eine Gewährleistung jedweder Art für die Vollständigkeit und die Richtigkeit, sowie für die Brauchbarkeit der in den Handreichungen enthaltenen Informationen übernehmen die DIS, deren Vertreter und Angestellte, sowie die beteiligten Verfasser nicht.

² ICT – *Information and Communication Technology* oder auch IKT – Informations- und Kommunikationstechnologie, https://de.wikipedia.org/wiki/Informations-_und_Kommunikationstechnik (dieser und alle weiteren Links zuletzt abgerufen am 24.5.2019).

4. Effizienzsteigerung durch ausschließlich elektronische Übermittlung von Unterlagen

Eine Einsparung an Zeit und Aufwand durch Nutzung elektronischer Kommunikationsmittel ist regelmäßig nur dann zu erwarten, wenn von der Übermittlung in körperlicher Form abgesehen wird. Ausgenommen hiervon sind Schiedssprüche. Eine Übermittlung von Schriftsätzen und Anlagen als Email-Anhang ist möglich, stößt aber bei größerem Datenvolumen an technische Grenzen sowie an Grenzen der Empfängerfreundlichkeit. Deshalb ist zumindest in mittleren bis größeren Schiedsverfahren die Nutzung eines Datenraums in der Cloud oder eine Verteilung per sFTP³-Server in Betracht zu ziehen.

Vorteilhaft ist die Nutzung des Formats PDF,⁴ vorzugsweise mit Texten die maschinenlesbar (texterkannt) sind. Gängige Formate für Kalkulationstabellen (zB .xls) oder Texte die im Verfahren bearbeitet werden müssen (zB .docx, .rtf für *Redfern Schedules*) sollten nicht ausgeschlossen werden. Andere Formate bedürfen der Abstimmung. Die Dateien müssen jeweils einen im Verfahren einmaligen Namen haben, der mit der in den Schriftsätzen benutzten Bezeichnung übereinstimmt und die Partei, welche das Dokument einreicht, erkennen lässt.

Die Übermittlung soll sicher erfolgen, wenn darauf nicht ausdrücklich verzichtet wird. Erfolgt die Übermittlung per Email, die nicht verschlüsselt ist, sollte eine Mindestsicherheit durch Packen der Anlagen in ein Dateiarchiv (ZIP, RAR, etc.) erfolgen, dass mindestens mit AES256⁵ oder besser verschlüsselt und durch ein Passwort gesichert ist.

5. Effizienzsteigerung durch Audio- und Videokonferenzen

Jedes persönliche Treffen im Schiedsverfahren erfordert, dass Beteiligte an- und abreisen. Das vergrößert das benötigte Zeitfenster und erschwert die Terminfindung. Zur Steigerung der Verfahrenseffizienz kann deshalb vorzugsweise von Treffen der Verfahrensbeteiligten abgesehen und Audio- oder Videokonferenzen abgehalten werden. Das gilt insbesondere für die Abstimmungen zum Verfahrensmanagement. In kleineren bis mittleren Schiedsverfahren mit vorhersehbar kurzer Verhandlungsdauer kann auch die mündliche Verhandlung per Videokonferenz mit einem gängigen Programm durchgeführt werden.

Auch wenn auf eine körperliche Präsenz der Verfahrensbeteiligten am Verhandlungsort nicht verzichtet wird, kann es effizienter sein, alle oder einzelne Zeugen oder Sachverständige per Videokonferenz zu befragen. Simultanübersetzer oder Dolmetscher können über eine Audiokonferenzschaltung ihre Dienstleistung erbringen.

Weil Audio- und Videokonferenzen über die Plattformen von Dienst Anbietern abgewickelt werden, ist auf deren Geschäftsbedingungen und Datenschutzregelungen zu achten und zwar vor allem bei besonderem Geheimhaltungsinteresse.

6. Protokollierung

Die Kosteneffizienz der Verhandlung kann durch einen digitalen Audiomittschnitt der Verhandlung gesteigert werden, aus dem allenfalls wesentliche Teile nachträglich transkribiert werden oder der insgesamt mittels Spracherkennung in Text umgesetzt wird.

Werden hierzu Dienstanbieter eingesetzt, ist auf deren Geschäftsbedingungen und Datenschutzregelungen zu achten und zwar vor allem bei besonderem Geheimhaltungsinteresse.

³ sFTP – *Secure File Transfer Protocol*, https://de.wikipedia.org/wiki/SSH_File_Transfer_Protocol.

⁴ PDF – *Portable Document Format*, https://de.wikipedia.org/wiki/Portable_Document_Format.

⁵ AES256 – *Advanced Encryption Standard 256*, https://de.wikipedia.org/wiki/Advanced_Encryption_Standard.

7. Datensicherheit

Daten- und Kommunikationssicherheit wird durch das schwächste Glied im System bestimmt. Erhöhte Sicherheitsanforderungen sind deshalb frühestmöglich im Verfahren zu klären; und zwar auf Grundlage einer realistischen Bedrohungsprognose. Auf dieser Basis sind alle Verfahrensbeteiligten auf das angemessene Maß an System- und Kommunikationssicherheit zu verpflichten sowie zur sofortigen Meldung von sicherheitsrelevanten Vorfällen in ihrer Sphäre, sowie ggf. zur Mitwirkung.

Datenkommunikation ist leicht durch Dritte angreifbar. Deshalb ist aufgrund der Bedrohungsanalyse zu entscheiden, ob und wie alle Daten (insbesondere Emails) verschlüsselt werden.

Verfahrensbeteiligte, die ihre Tätigkeit im Verfahren nicht unter ausschließlicher Nutzung einer Systemarchitektur entfalten, die professionell technisch zureichend gegen Bedrohungen gesichert und in der eine Nutzerverwaltung mit Zugriffsrechten und Passwortmanagement etabliert ist, müssen jedenfalls ihren Rechner und Netzzugang mit ausreichendem Passwort und Zugriffsschutz versehen und die das Verfahren betreffenden Daten zureichend verschlüsselt vor dem technischen und auch körperlichen Zugriff unbefugter Dritter sichern.

8. Schutz personenbezogener Daten

Die Datenschutz-Grundverordnung (DSGVO) nimmt Schiedsverfahren nicht von ihrem Anwendungsbereich aus. Nur zwingend benötigte personenbezogene Daten sollen ins Verfahren eingeführt werden. Die Parteien tragen dafür Sorge, dass von ihnen jeweils ins Verfahren eingeführte personenbezogene Daten keiner Zustimmung für die Zwecke der Verfahrensdurchführung bedürfen oder die erforderliche Zustimmung vorliegt.

Um die Menge personenbezogener Daten, deren Kenntnis nicht für die Rechtsverfolgung oder Rechtsverteidigung unerlässlich ist, im einzelnen Verfahren möglichst klein zu halten, kann die Partei, welche sie erstmals in das Verfahren einführt, alle derartigen Daten zB anonymisieren (schwärzen) oder mit Pseudonymen versehen. Dies erfolgt unter dem Vorbehalt, dass das Schiedsgericht die Offenlegung der entpersonalisierten Daten anordnen kann, wenn das sich als zweckmäßig erweist.

Besteht zu einzelnen solcher Daten seitens der sie einführenden Partei Unsicherheit, ist das den empfangenden Verfahrensbeteiligten erläuternd mitzuteilen. Datenschutzbrüche sind den anderen Beteiligten sofort zu melden. Die grundsätzlich relevante Frage des Zeitpunkts der Löschung aller Daten im Schiedsverfahren auf allen Datenträgern einschließlich des Datenraums (Aktenvernichtung) ist so zu klären, dass sie frühestmöglich, regelmäßig bei Ablauf gesetzlicher Aufbewahrungsfristen, vollständig erfolgt.

Werden im Verfahren personenbezogene Daten in Territorien außerhalb der EU übermittelt, gespeichert oder verarbeitet, sind die gesetzlich geforderten Vorkehrungen zuvor regelmäßig zu treffen.

II. Praktischer Leitfaden zu Anlage 3 lit. G 2018 DIS-Schiedsgerichtsordnung

1. Zweck

Zweck dieses Abschnitts ist es, nach Maßgabe der Verfahrensregeln mit Hilfe der Nutzung heute verfügbarer, konkret benannter technischer Mittel möglichst unkomplizierte und den Bedürfnissen der Verfahrensbeteiligten Rechnung tragende Vorgehensweisen zur sicheren Nutzung der Informations- und Kommunikationstechnik in DIS-Schiedsverfahren an die Hand zu geben. Diese sollen es ermöglichen, auf die Erstellung und Übermittlung körperlicher Dokumente zu verzichten, sofern dies gewünscht und rechtlich möglich ist. Das erfolgt auch mit Blick auf die Kommunikations- und Datensicherheit. Das Thema Schutz personenbezogener Daten wird hier allenfalls gestreift.

Dem Leser soll ein einigermaßen anwendungsnahe Grundverständnis der technischen Möglichkeiten digital und papierlos geführter Schiedsverfahren gegeben werden. Dieses kann und soll keinesfalls den Einsatz geschulter und erfahrener ICT-Mitarbeiter entbehrlich machen, sondern in die Lage versetzen, in einen Dialog mit „eigener“ ICT zu treten und das volle Potenzial digitaler Aktenführung und Kommunikation für ein effizientes Schiedsverfahren zu nutzen.

2. Themenfolge

Die Darstellung der technischen Mittel zur effizienteren Verfahrensführung mittels ICT folgt dem zeitlichen Ablauf des Verfahrens, dh den Verfahrensstadien in denen die jeweilige Aufgabe sich technisch stellt. So wenden sich die Abschnitte 3-4 unten zunächst in erster Linie an die Parteien. Abschnitt 4 wendet sich auch an Schiedsrichter, Abschnitt 5 vor allem an Schiedsrichter. Abschnitte 6-7 richten sich vornehmlich an Schiedsrichter aber auch die Parteien. Abschnitt 8 betrifft Dreierschiedsgerichte. Abschnitt 9 richtet sich an alle Verfahrensbeteiligten. Die Abschnitte 10 und 11 richten sich an das Schiedsgericht und betreffen dessen verfahrensleitende Tätigkeit, die durch die Anlagen 1 und 2 vereinfacht werden soll.

3. Aktenbestandteile in digitalem Format

Schreiben, Schriftsätze und deren Anlagen nur digital auszutauschen erhöht die Verfahrenseffizienz grundsätzlich, weil die Erstellung gedruckter Unterlagen und deren körperliche Versendung zusätzliche Arbeitsschritte und mehr Übermittlungsaufwand nach sich zieht. Demgegenüber sind die meisten Dokumente bei den Parteivertretern und ihren Mandanten heute von Anfang an elektronisch gespeichert und elektronisch in Augenblicken zu Minimalkosten übermittelbar. Wo das nicht der Fall ist, kann eine Digitalisierung durch Scannen jedenfalls beim Parteivertreter mit den dort regelmäßig vorhandenen Multifunktionsgeräten einfach erfolgen. Allerdings erfordert die Übermittlung an Schiedsgericht und die anderen Parteien Vorkehrungen, damit Aktenbestandteile leicht gelesen und ohne Schwierigkeiten zugeordnet, gespeichert und verarbeitet werden können. Hierzu ist Folgendes zu beachten.

a) Formate

Die Standardisierung von elektronischen Dateien ist heute so weit fortgeschritten, dass die Nutzung typischerweise in Büros weltweit eingesetzter Datenformate keine technischen Probleme mehr aufwirft. Weil das Format PDF sicherer als andere Datenformate die ursprüngliche grafische Darstellung wiedergibt und auch Funktionen wie die Einbettung von Bildern/Fotos sowie auch gewisse Sicherheitsfunktionen anbietet, hat sich dieses Format für Aktenbestandteile in Schiedsverfahren jeder Art etabliert.

Dateien in von Textverarbeitungs- (zB .doc, .docx oder .rtf⁶) oder Tabellenkalkulationsprogrammen (zB .xls) generierten Formaten sind gleichwohl zweckmäßig, wenn eine sequentielle Bearbeitung durch die Verfahrensbeteiligten erforderlich ist (zB *Redfern Schedules*) oder Berechnungen mit ggf. variierenden Daten vorgenommen oder nachvollzogen werden müssen. Zu achten ist dann allerdings darauf, dass die Dateien von allen Verfahrensbeteiligten mit dem gleichen (niedrigen) Aufwand geöffnet, gelesen und bearbeitet werden können. Daher sollte auf Nischenformate (zB Apples Textverarbeitung *Pages* [.pages]) möglichst verzichtet werden.

Andere Dateiformate für Foto- oder Grafikdateien, Tonaufzeichnungen, Videosequenzen sind unproblematisch, wenn für sie gängig und regelmäßig die zur Anzeige erforderlichen Programme auf üblichen Computern installiert sind.

⁶ Zu Dateiformaten s. https://de.wikipedia.org/wiki/Liste_von_Dateinamenserweiterungen.

Dateiformate, die nur von speziellen, nicht allgemein verfügbaren Programmen, wie CAD⁷-Programmen oder Programmen zur Verzögerungsanalyse (Bauprojekte) verwendet werden, bedürfen jedenfalls einer besonderen, angemessenen Regelung unter den Verfahrensbeteiligten, bevor sie verwendet werden. Falls es nur um die optische Darstellung der Inhalte einer solchen Programmdatei geht, kann es ratsam sein, den Inhalt in eines der gängigeren Formate (idealerweise PDF) zu exportieren.

Um die einfache Weiterverarbeitung dieser elektronischen Aktenbestandteile zu gewährleisten, sollte unter allen Beteiligten eine entsprechende einheitliche Formatnutzung vereinbart oder festgelegt werden.

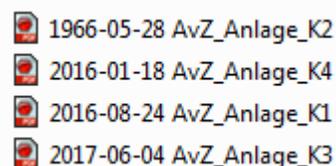
b) Bezeichnung und Organisation digitaler Aktenbestandteile

Einer gespeicherten Datei sieht man ihren Inhalt anders als bei gedruckten Unterlagen im Aktenordner nicht auf den ersten Blick an. Deshalb ist es wichtig, dass der Name, der der Datei gegeben wird, die Information enthält, die notwendig ist, um zu erkennen, worum es sich handelt. Da Betriebssysteme heute längere und freier gestaltete Dateinamen verwalten können als früher, besteht hier Gestaltungsspielraum. In der Praxis hat sich hierzu bewährt, den Dateinamen entsprechend den Bezeichnungen bei gedruckten Schriftsätzen zu vergeben. Wesentlich ist nur, dass jeder Dateiname auch bei neuen, überarbeiteten Versionen nur einmal vergeben wird; und zwar nach einer einheitlichen, anfangs gewählten Systematik. Also bspw. für eine Schiedsklage mit Anlagen wie folgt abgebildet:



AvZ_Schiedsklage_07112018
AvZ_Anlage_K4
AvZ_Anlage_K3
AvZ_Anlage_K2
AvZ_Anlage_K1

Um automatische historische Beweisunterlagen in chronologischer Reihenfolge und nicht in der Folge der Anlagenbezeichnungen sortieren zu können, kann deren Datierung dem eigentlichen Dateinamen vorangestellt werden.



1966-05-28 AvZ_Anlage_K2
2016-01-18 AvZ_Anlage_K4
2016-08-24 AvZ_Anlage_K1
2017-06-04 AvZ_Anlage_K3

Eine sinnvolle Sortierung wird dabei nur erreicht, wenn das Datum im Format „Jahr-Monat-Tag“ angegeben wird, also nicht zB im in Deutschland gängigen Format „24.11.2018“ oÄ.

Allerdings sollten bei alledem für Dateinamen 32 (Abwärtskompatibilität) bzw. 255 Zeichen nicht überschritten und keine Sonderzeichen verwendet werden.

Um die weitere Nutzung der Dateien im Verfahren nicht unnötig zu erschweren, sollen mehrere getrennte Originale nicht in einer einzigen Datei, wie nachfolgend abgebildet



AvZ_Schiedsklage_u_Anlagen_1_66_07112018

⁷ CAD – Computer Aided Design, s. <https://de.wikipedia.org/wiki/CAD>.

zusammengefasst und ebenso wenig mit maschinengenerierten Dateibezeichnungen wie nachfolgend abgebildet



verwendet werden. Wurden diesen Empfehlungen nicht befolgt, gibt es Abhilfe. So können PDF-Dateien mittels gängiger Bearbeitungsprogramme⁸ oder teilweise mit Werkzeugen des Betriebssystems seitenbezogen in mehrere Teile aufgespalten werden, sodass Einzeldateien entstehen. Dateien können auch mit Hilfsprogrammen⁹ in einer einheitlichen Operation strukturiert umbenannt werden.

c) *Qualität und Maschinenlesbarkeit von digitalen Kopien*

In vielen Fällen werden Parteivertreter Dokumente, die ihnen nicht digital vorliegen, mit einem büroüblichen Multifunktions- oder Dokumentenscanner digitalisieren. Dabei sollte zunächst auf eine ausreichend hohe Qualität des Scans geachtet werden. Die Scanqualität wird bei handelsüblichen Geräten in *dots per inch* (dpi¹⁰) angegeben und kann meist in Stufen von 100 dpi gewählt werden. Normal groß gesetzte Textdokumente sollten mit einer Qualität von 200-300 dpi digitalisiert werden. Dokumente mit kleiner gesetztem Text wie bspw. AGB, Zeichnungen und dergleichen sollten eher mit einer höheren Auflösung digitalisiert werden.

Texte, die digital erfasst werden, sollten zudem – und dies ordnen bereits viele Schiedsgerichte ausdrücklich an – nach dem Scanvorgang nachbearbeitet werden, sodass der enthaltene Text mittels OCR¹¹ maschinenlesbar wird. Manche Dokumentenscanner oder Multifunktionsgeräte liefern diese Option bereits mit, wenn sie beim Scanvorgang gewählt wird. In allen anderen Fällen – und insbesondere auch, wenn eine digitale Kopie vom Mandanten bereitgestellt und noch nicht texterkannt wurde, – ermöglicht entsprechende Software¹² auch die Nachbearbeitung beim Empfänger. Durch diesen Arbeitsschritt erhält das digitalisierte Dokument für die Verfahrensbeteiligten einen Mehrwert, auf den auch immer mehr Schiedsgerichte Wert legen: Es kann mittels der Suchfunktion zB der gängigen PDF-Leseprogramme – zT auch Dateiübergreifend – nach Begriffen gesucht werden. Allerdings wird die Qualität der Suchergebnisse durch die Qualität der Vorlage und die Erkennungsgenauigkeit beeinflusst. Es gibt stets eine gewisse Fehlerrate.

4. **Übermittlung von digitalen Aktenbestandteilen**

Bei der Kommunikation mit der DIS ist stets Art. 4.1 2018 DIS-Schiedsgerichtsordnung zu beachten. Mit Ausnahme der Zustellung der Schiedsklage und des Schiedsspruchs sowie vor Bildung des Schiedsgerichts ggf. (wenn keine Vereinbarung der Parteien zur digitalen Kommunikation vorliegt) Klageerweiterung und Widerklage können alle Aktenbestandteile lediglich in elektronischem Format und mittels Datenübertragung an die weiteren Verfahrensbeteiligten übermittelt werden; und zwar jedenfalls dann, wenn das vereinbart ist oder solange kein Widerspruch dagegen erhoben wurde oder soweit alle Verfahrensbeteiligten diese Form der Kommunikation praktizie-

⁸ Bspw. *Adobe Acrobat, PDF Expert, PDFPen, Docscorp, PDFDocs* uvm.

⁹ Bspw. *Ant Renamer* <http://antp.be/software/renamer>; *ReNamer* <http://www.den4b.com/products/renamer> uvm.

¹⁰ DPI – *Dots Per Inch*, <https://de.wikipedia.org/wiki/Punktdichte>.

¹¹ OCR – *Optical Character Recognition*, s. <https://de.wikipedia.org/wiki/Texterkennung>.

¹² Bspw. *Adobe Acrobat, Abbyy FineReader, DocsCorp PDFDocs, Readiris, Omnipage*, vgl. für weitere https://en.wikipedia.org/wiki/Comparison_of_optical_character_recognition_software.

ren. Im Regelfall wird dies nach Anhörung der Parteien vom Schiedsgericht in der ersten verfahrensleitenden Anordnung ausdrücklich geregelt.

Heute wird in Schiedsverfahren die Kommunikation per Email, der ggf. die Schreiben, Schriftsätze nebst Anlagen beigelegt sind, auch zu Zwecken fristwahrender Eingaben praktiziert. Ob auf die zeitgleiche körperliche Versendung verzichtet wird, ist im einzelnen Schiedsverfahren zu klären, aber grundsätzlich sinnvoll, wenn und solange daraus keine Komplikationen erwachsen. Letzteres ist zumindest bei internationalen Verfahren im Rahmen einer fairen Prognose einzelfallbezogen abzuwägen, bevor ausschließlich elektronisch kommuniziert wird.

Die beschriebene Kommunikation per Email ist grundsätzlich – ohne Verschlüsselung – unsicher, da mit technischen Mitteln „einsehbar“. Sie ist in der praktizierten Form der Beifügung einer Vielzahl von Dateianhängen auch aus Sicht der Empfänger unpraktisch. Zu beachten ist auch, dass eingesetzte „Spamfilter“¹³ dazu führen können, dass Email-Sendungen nicht in den Email-Client von intendierten Empfängern gelangen, wenn diese nicht im Spamfilter auf eine sogenannte „White List“ gesetzt wurden.

Zudem ist, wo immer Dienste für die digitale Dokumentenübermittlung genutzt werden (also sowohl bei der Kommunikation per Email als auch bspw. bei der Nutzung von Datenräumen und Cloud-Anbietern), zu bedenken, dass nur eine Verschlüsselung vor der unbefugten Kenntnisnahme durch Dritte einen gewissen Schutz bietet. Die dabei nutzbaren Verschlüsselungstechnologien werden in Zusammenhang mit den zur Verfügung stehenden Diensten nachfolgend angesprochen.

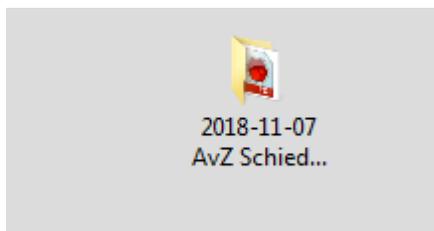
Hält man der Einfachheit halber an der Übermittlung per Email fest, können die oben beschriebenen Nachteile mit verschiedenen Maßnahmen vermieden werden, die nun angesprochen werden.

a) *Verwendung eines „Containers“ für Schriftsätze und deren Anlagen*

Die Handhabung einer Vielzahl von gleichzeitig übermittelten Dateien wird vereinfacht, wenn sie in ein Dateiarchiv in einem gängigen Kompressionsformat (regelmäßig .zip¹⁴) gepackt werden, das auch das Gesamtvolumen komprimiert. Gängige Betriebssysteme wie *Windows*, *iOS* oder *Linux* verfügen hierzu von Hause aus im Auslieferungszustand über Werkzeuge. Jedoch sind wegen des größeren Funktionsumfangs Spezialprogramme¹⁵ zu empfehlen, die zu lizenzieren wenig oder nichts kostet. Hierzu werden die zu übermittelnden Dateien auf dem Desktop in ein Verzeichnis kopiert, das dann bspw. zu einer ZIP-Datei komprimiert wird. Es ist auch möglich, in diesem Verzeichnis¹⁶ Unterverzeichnisse (Ordner) anzulegen.

Beispiel:

(i)



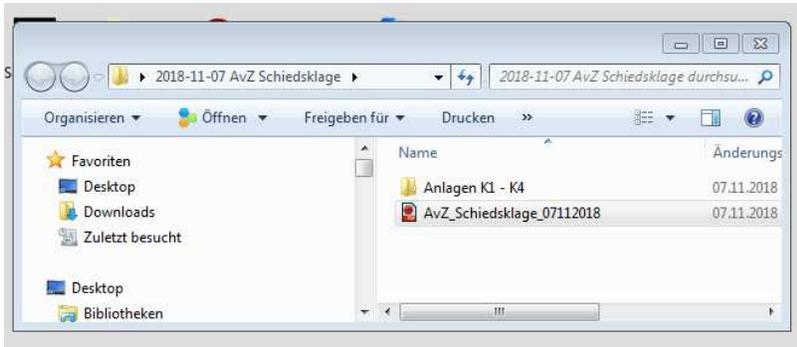
¹³ S. hierzu <https://de.wikipedia.org/wiki/Spamfilter>.

¹⁴ ZIP – Dateiformat <https://de.wikipedia.org/wiki/ZIP-Dateiformat> aber ggf. auch andere Formate wie RAR [https://de.wikipedia.org/wiki/RAR_\(Dateiformat\)](https://de.wikipedia.org/wiki/RAR_(Dateiformat)), TAR [https://de.wikipedia.org/wiki/Tar_\(Packprogramm\)](https://de.wikipedia.org/wiki/Tar_(Packprogramm)), s. auch https://de.wikipedia.org/wiki/Liste_von_Datenkompressionsprogrammen.

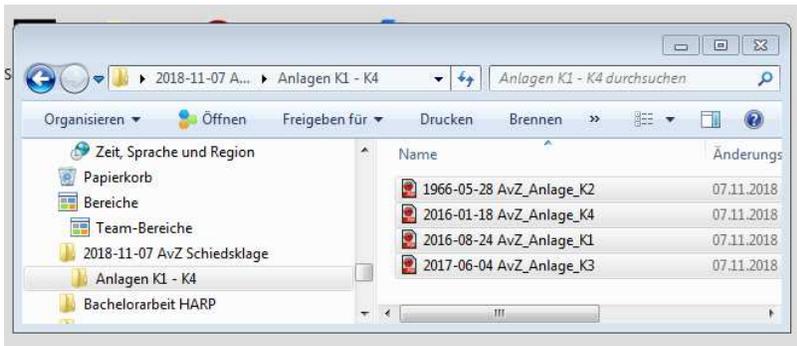
¹⁵ Bspw. *WinZip* oder *7ZIP* uvm.

¹⁶ Dateiverzeichnis ist Teil des Dateisystems, <https://de.wikipedia.org/wiki/Dateisystem>.

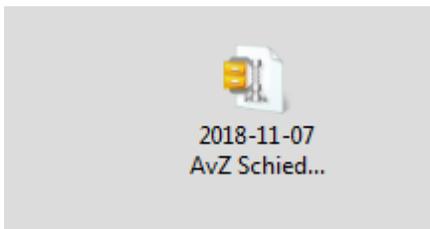
(ii)



(iii)

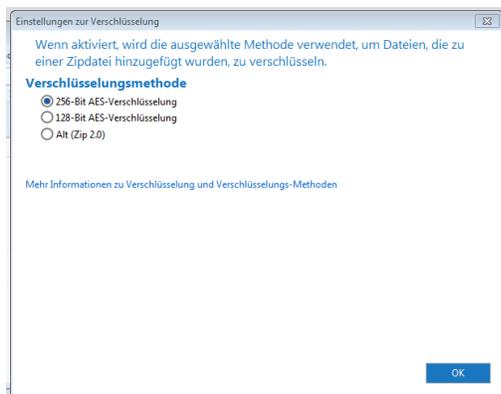
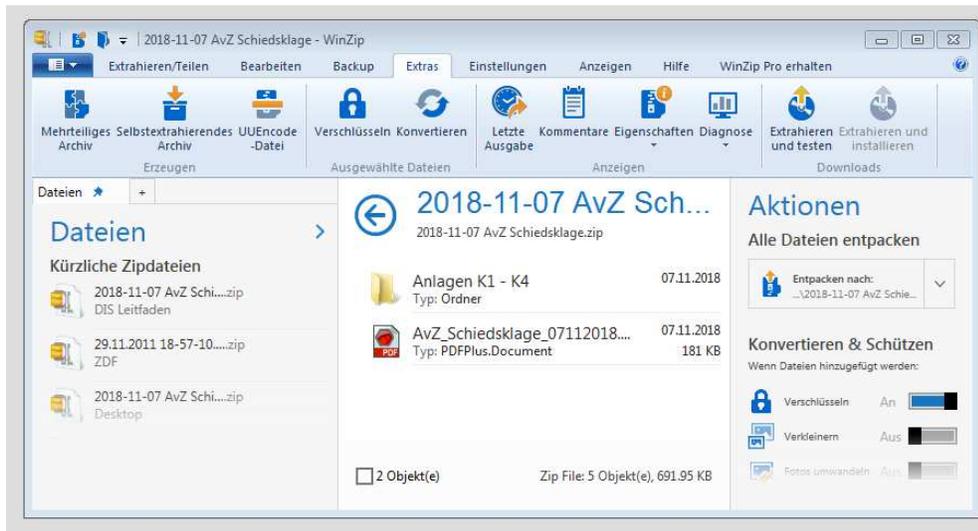


(iv)



Es ist weiter möglich, die Dateien in dem ZIP-Archiv durch ein Passwort (siehe II.9.a)(e)) zu sichern. Dabei ist darauf zu achten, dass das ZIP-Programm eine ausreichend sichere¹⁷ Verschlüsselung einsetzt.

¹⁷ BSI – Empfehlungen zu Kryptographie, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102.pdf?__blob=publicationFile, 15.



Das Passwort sollte nicht auf dem gleichen Kanal übermittelt werden, also nicht per Email, sondern auf einem anderen Kanal, wie zB (fern-)mündlich oder per SMS.¹⁸ Dies gewährleistet ein wünschenswertes Minimum an Sicherheit und Wahrung der Vertraulichkeit.

Insbesondere – aber nicht ausschließlich – dann, wenn man einen sogenannten „eBrief“ (einen Schriftsatz, in den Hyperlinks zu den Anlagen eingebettet sind, was eine Beibehaltung der Verzeichnisstruktur beim Empfänger erfordert) übermitteln will, kann es zweckmäßig sein, die Verzeichnisstruktur mit den Dateien auf ein sogenanntes „Disk-Image“¹⁹ zu kopieren, wie man es auch zum Brennen von CDs oder DVD-Disks²⁰ benutzt. Programme hierfür sind als *Shareware* oder *Open Source* Anwendungen zu erhalten. Wegen der Containerverschlüsselung sollten auch diese in ein passwortgeschütztes ZIP-Archiv gepackt werden.

b) Größe der Nachrichten einschl. Anhang

Bei dem Versand von Schriftsätzen und Anlagen über Email²¹ kommt es oft vor, dass eine Email vom Empfangsserver eines der Verfahrensbeteiligten abgelehnt wird, weil sie die zulässige Gesamtgröße für eingehende Kommunikation überschreitet. Zwar nutzen viele Verfahrensbeteiligte professionelle Mailserver zB einer Kanzleiinfrastruktur, dennoch werden Emails mit mehr als 20 MB²² Datenvolumen oftmals abgelehnt. Sicherheitshalber sollte der Versand entsprechend großer Dateikonvolute daher von vorne herein auf mehrere Emails aufgespalten werden. Dabei

¹⁸ SMS – *Short Message Service*, https://de.wikipedia.org/wiki/Short_Message_Service.

¹⁹ ISO-Abbild, <https://de.wikipedia.org/wiki/ISO-Abbild>.

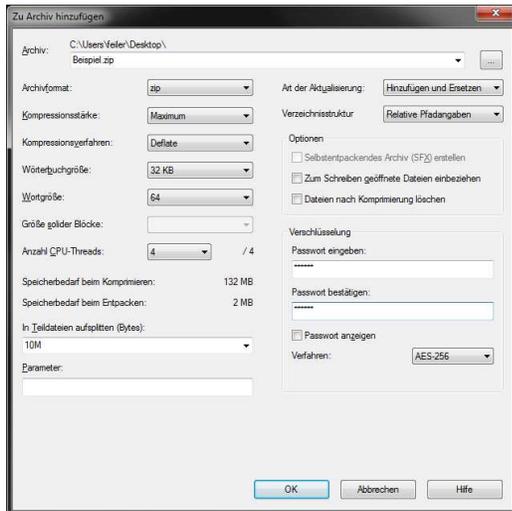
²⁰ S. hierzu https://de.wikibooks.org/wiki/Computerhardware:_CD_und_Nachfolger.

²¹ S. zu Email zB https://de.wikibooks.org/wiki/Internet:_E-Mail:_Protokolle.

²² MB – *Mega Byte*, https://de.wikibooks.org/wiki/Computerhardware:_Speicher.

sollte, um den Empfängern die Zuordnung zu erleichtern, mit eindeutigen Betreffzeilen („part 1/3“, „part 2/3“ usw.) gearbeitet werden und in der ersten Email ein Hinweis auf die folgenden Paketeile enthalten sein („...übermitteln wir mit dieser und nachfolgenden weiteren 2 Emails...“).

Durch die Verwendung eines Programms zum Archivieren der Dateien als ZIP-Datei kann auch auf Größenbeschränkungen gut eingegangen werden: Gängige Programme bieten beim Erstellen des ZIP-Containers nämlich an, diesen in mehrere Container einer maximalen Größe X aufzuspalten.



Im Beispiel weist der Bearbeiter das Programm an, Archive in Teildateien von 10 MB aufzuspalten und mit einem Passwort zu versehen.

c) Verschlüsselung der Nachrichten

Der Verschlüsselung von Kommunikation kommt naturgemäß insbesondere im Schiedsverfahren eine hohe Bedeutung zu. Bei Emails wird dabei zwischen Verschlüsselung im Transit (dh während der Übertragung der Email von einem Server²³ zum nächsten) und Verschlüsselung *in situ*, dh im auf dem Server ruhenden, abgelegten Zustand, unterschieden.

Heute schützen oft verschiedene Werkzeuge im Hintergrund Email-Nachrichten im Transit. Verfügen alle Verfahrensbeteiligten über eine eigene Domain und administrieren ihren eigenen Email-Server, können sie den Email-Verkehr mit dem TLS-²⁴Protokoll durch ihre Administratoren sichern lassen. Auch viele externe Anbieter von Email-Postfächern unterstützen inzwischen standardmäßig die TLS-Verschlüsselung. Allerdings verschlüsselt das TLS-Protokoll die Daten nur während des Transports, sie werden damit regelmäßig auf Servern entschlüsselt liegen, die der Kontrolle der Verfahrensbeteiligten entzogen sind. Zudem leiten (insbesondere bei Mobilgeräten) viele Programme und Apps zur Email-Kommunikation die Nachrichten zur Gewährleistung zusätzlicher (Komfort-)Funktionen über weitere Server in der Cloud, wo ebenfalls Zugriff auf sämtliche Nachrichten besteht und auf denen teilweise über längere Zeiträume Kopien liegen.²⁵

Wenn nicht alle Beteiligten auf Verschlüsselung ganz verzichten, sind aus Sicherheitsgründen sowie jedenfalls bei Beteiligung von in Deutschland zugelassenen Anwälten auch aus berufsrechtlichen Gründen zusätzliche Verschlüsselungsmaßnahmen in Betracht zu ziehen.

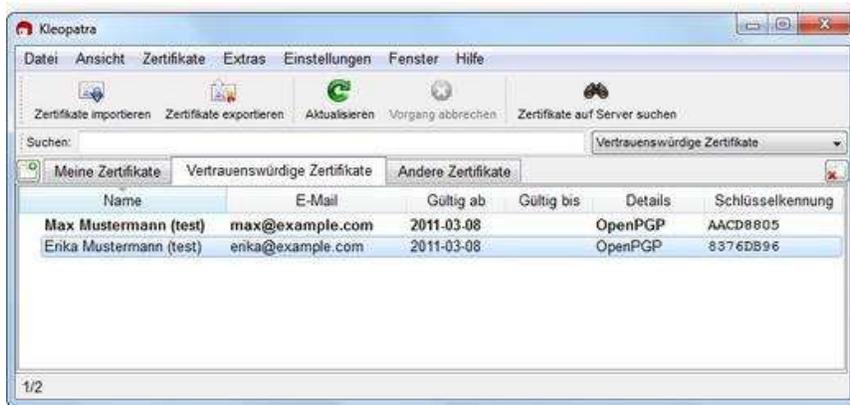
Dazu hat sich die sogenannte „asymmetrische Verschlüsselung“ bewährt, bei der jeder Kommunikationsteilnehmer über einen privaten, nicht geteilten Schlüssel zum Entschlüsseln der an ihn ge-

²³ Mailserver <https://de.wikipedia.org/wiki/Mailserver>.

²⁴ TLS – *Transport Layer Security*, https://de.wikipedia.org/wiki/Transport_Layer_Security.

²⁵ So bspw. die *iOS-* und *Android Apps Microsoft Outlook, BlueMail, Spark* uvm.

richteten Nachrichten verfügt, sowie einen öffentlichen Schlüssel, den er mit allen anderen Teilnehmern teilt und den diese zum Verschlüsseln benutzen. Vorausgesetzt, die Teilnehmer können sicher sein, dass sie jeweils die authentischen öffentlichen Schlüssel des Adressaten ihrer Nachrichten kennen, brauchen die Schlüssel aus technischer Sicht nicht zertifiziert sein (zB von der Bundesnotarkammer). Wenn die Verfahrensbeteiligten alle deutsche Rechtsanwälte sind, können sie das BeA²⁶ benutzen, das eine Sicherheitsarchitektur bereitstellt. Dies wird in Schiedsverfahren aber nicht stets der Fall sein, sei es, weil Parteien außerhalb des deutschen Rechtsraums am Verfahren beteiligt sind, oder weil Schiedsrichter oder andere Verfahrensbeteiligte nicht als Rechtsanwalt zugelassen sind. Ebenso wird nicht allen Beteiligten am Arbeitsplatz bereits eine geeignete interoperable Verschlüsselungstechnologie zur Verfügung stehen. Deshalb wird nachfolgend anhand einer *Open-Source*-Lösung (es gibt viele, auch kommerzielle, Produkte) dargestellt, wie für das einzelne Verfahren eine Verschlüsselung *End-to-End*²⁷ gewährleistet werden kann; nämlich das Open PGP²⁸ implementierende, vom BSI beauftragte, *Paket Gpg4win*,²⁹ das in Email-Clients, wie dem verbreiteten *Outlook*, durch Plug-Ins (GpGOL³⁰) integrierbar ist.



Nach der einfachen Installation am Arbeitsplatz erzeugt jeder Verfahrensbeteiligte sein Paar aus öffentlichem und privatem Schlüssel. Sodann werden unter allen Beteiligten die öffentlichen Schlüssel in Dateiform ausgetauscht und dann in *Kleopatra* (eine Programmkomponente von *Gpg4win*) importiert. Alle Beteiligten oder allein das Schiedsgericht können dann die Schlüssel verwenden, und – soweit gewünscht – als authentisch, also vertrauenswürdig mit ihrer in *Kleopatra* verwalteten, digitalen Signatur zertifizieren. Die verschlüsselte Versendung kann dann mit zB GpGOL unkompliziert direkt aus *Outlook* vorgenommen und die Nachricht beim Empfänger entschlüsselt werden.

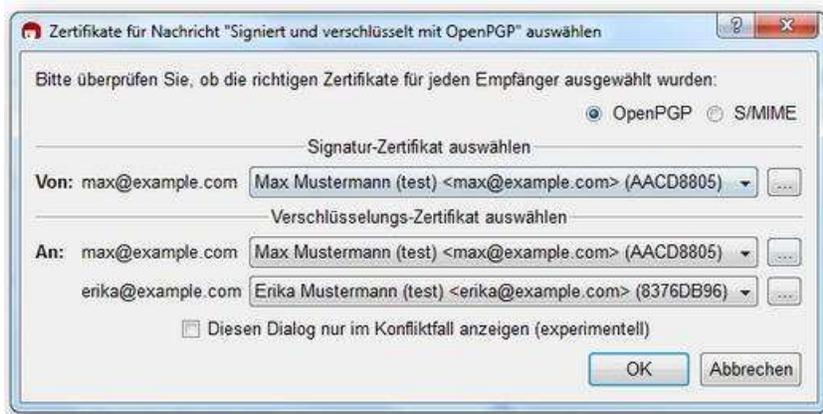
²⁶ BeA, <https://bea.brak.de/>.

²⁷ S. weiterführend https://de.wikibooks.org/wiki/IT-Sicherheit_f%C3%BCr_Privatanwender:_Grunds%C3%A4tze:_Transportverschl%C3%BCsslung.

²⁸ PGP – *Pretty Good Privacy*, https://de.wikipedia.org/wiki/Pretty_Good_Privacy.

²⁹ https://www.bsi.bund.de/DE/Themen/Kryptografie_Kryptotechnologie/Kryptotechnologie/Gpg4win/gpg4win_node.html Gpg4win <https://www.gpg4win.de/>; <https://de.wikipedia.org/wiki/PGP/MIME>, das die GUI (*Graphical User Interface*, https://de.wikipedia.org/wiki/Grafische_Benutzeroberfl%C3%A4che) *Kleopatra* beinhaltet.

³⁰ GpGOL, https://de.wikibooks.org/wiki/GnuPG:_Installation.



Wie stets bei Computerprogrammen ist zur Installation und zum Erlernen der Handhabung etwas Zeit notwendig, die sich hier aber in Grenzen halten sollte.

Sollte die Installation von PGP und den zugehörigen Programmen nicht möglich sein, kann auch alternativ auf ein weiteres Übermittlungsverfahren mittels asymmetrischer Verschlüsselung namens S/MIME³¹ zurückgegriffen werden. Hierfür müssen die Beteiligten ebenfalls über ein Schlüsselpaar mit privatem und öffentlichem Schlüssel verfügen, welches – und darin liegt wiederum eine mögliche Schwachstelle – jedoch von einem Anbieter erzeugt wird. Die in Büroumgebungen gängigen Mailprogramme können mit dieser Art der Verschlüsselung meist ohne Zusatzsoftware umgehen, je nach Kanzlei-Infrastruktur ist eine Konfiguration des Kanzlei-Mailserverns notwendig.

Es ist möglich, die öffentlichen Schlüssel per Email auszutauschen (was dann aber noch unverschlüsselt erfolgt), wenn sie nicht bereits auf einem vertrauenswürdigen dedizierten Server liegen. Wer hier Angriffspunkte durch „*Man in the Middle*“-Angriffe³² vermeiden will, tauscht die öffentlichen Schlüssel körperlich auf einem Datenspeicher (*Flash-Memory*³³-Stick) persönlich aus. Postversand ist möglich, aber auch angreifbar.

Am Rande sei noch bemerkt: Auch die heute gängigen mobilen Anwendergeräte (*Smartphones*, *iPads*³⁴) können mit verschlüsselten Emails entweder herstellereitig oder nach Installation einer Zusatzsoftware umgehen. S/MIME-Verschlüsselung beherrschen die genannten gängigen Betriebssysteme für Mobilgeräte ebenfalls. Der Verweis auf mobile Geräte ist also für sich gesehen noch kein Grund, sich gegen eine zusätzliche Sicherheitsstufe zu entscheiden.

d) Verteilung von Schriftsätzen über FTP-Server

Oft sind Email-Server so konfiguriert, dass das Datenvolumen einer Email begrenzt ist. Dieses Volumen wird bei der Übermittlung von umfangreichen Dateianhängen – wie oben beschrieben – leicht überschritten. Damit die Dateianhänge trotzdem übermittelt werden können und die obigen Maßnahmen zum aufgeteilten Senden nicht notwendig werden, werden FTP-Server³⁵ genutzt. Der Empfänger benötigt dann neben seinem Email-Programm noch einen sogenannten „Internetbrowser“ der – wie es heute Standard ist – über eine Funktion zum Herunterladen von Dateien via FTP verfügt. Die Empfänger erhalten per Email einen sogenannten „Downloadlink“,³⁶ den sie ankli-

³¹ S/MIME – *Secure/Multipurpose Internet Mail Extension*, s. <https://de.wikipedia.org/wiki/S/MIME>.

³² S. hierzu zB <https://de.wikipedia.org/wiki/Man-in-the-Middle-Angriff>, https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/g/g05/g05143.html.

³³ *Memory-Speicher*, <https://de.wikipedia.org/wiki/Flash-Speicher>.

³⁴ Für *Apple iOS (iPhone/iPad)* steht bspw. die App *iPGMail* bereit, auf *Android-Smartphones* kann *K9* zum Einsatz kommen.

³⁵ FTP – *File Transfer Protocol*, https://de.wikipedia.org/wiki/File_Transfer_Protocol.

³⁶ Downloadlink, <https://de.wikipedia.org/wiki/Hyperlink>.

cken, um dann über ihren Browser die Datei(en) auf ihren Arbeitsplatzrechner herunterzuladen. Es gibt Lösungen, bei denen der Download ohne Eingabe eines Benutzernamens (bspw. und oft die Email-Adresse des Adressaten) und eines Kennworts möglich ist. Für Schiedsverfahren sollte aber unbedingt eine Lösung genutzt werden, die ein Passwort erfordert.

Versender müssen hier über den Zugang zu dem FTP-Server verfügen und über die Software, welche den Upload der Datei auf diesen ermöglicht, sowie die einfache Generierung des Downloadlinks, die Passwortgenerierung und das anschließende Versenden an den oder die Adressaten. Viele Anwaltskanzleien betreiben einen eigenen FTP-Server, es gibt aber auch Dienstleister, die diesen Service anbieten. Allerdings können die Dienste von Datenräumen in der Cloud genutzt werden (siehe unten II.4.e), die gegenüber FTP verschiedene Vorteile bieten. Das Hochladen und die Hyperlinks können mit Plug-In für gängige Email-Clients vom Versender verwaltet werden. Diese werden anfänglich eine gewisse Einarbeitungszeit benötigen. Da insbesondere für das Schiedsgericht nicht transparent nachvollziehbar ist, ob alle Adressaten die Dateien erfolgreich auf den Arbeitsplatz heruntergeladen haben, sollte festgelegt werden, dass die Empfänger dies per Email quittieren müssen.

Grundsätzlich empfiehlt sich auch für die Übermittlung per FTP-Server die Verwendung eines Containers (ZIP-Archiv). Da das Herunterladen im Hintergrund abläuft, und nicht für jede einzelne Datei ein getrennter Download erfolgen muss, fallen längere Übertragungszeiten hier nicht wirklich ins Gewicht.

Jedoch sind bei Verwendung dieses Übermittlungsverfahrens Sicherheitsaspekte zu berücksichtigen. Weil das FTP-Protokoll keine Verschlüsselung im Transit vorsieht, sollte es nur als sFTP mit TLS und Zertifikaten³⁷ eingesetzt werden. Hinzu kommt: Wenn zB der Zugang zum FTP-Server unsachgemäß nicht passwortgeschützt und möglichst mit Mehrfaktoren-Authentifizierung gesichert ist, kann jeder, der sich Zugang zu dem Hyperlink verschafft, die Dateien herunterladen; und zwar ohne, dass dies den Verfahrensbeteiligten erkennbar wird. Nur der Administrator kann aus der Logdatei des FTP-Servers Informationen zu den Downloadvorgängen entnehmen, die aber regelmäßig technischer Natur sind, wie IP-Adressen³⁸ oder Datum und Uhrzeit des Zugriffs. Ebenso ist nur für den Serveradministrator transparent, wie lange die Dateien tatsächlich auf dem FTP-Server gespeichert sind, ob Sicherungskopien existieren und ob die Dateien unverändert geblieben sind, sowie wer unter welchen Umständen sonstige Zugriffsrechte hat (siehe hierzu auch unten Abschnitt II.9). Zudem können die Verfahrensbeteiligten nicht wie der Systemadministrator „sehen“, welche Dateien auf dem Server im Verzeichnis liegen. Sie sind „unsichtbar“. Vor allem bei kostenlos angebotenen FTP-Diensten stellen sich also Sicherheits- und Datenschutzfragen. Hinzu kommt, dass das *File Transfer Protocol* in seiner Grundausführung die Daten während des Transports nicht verschlüsselt. Es sollte daher darauf geachtet werden, dass eines der neueren, gängigen Verfahren zum verschlüsselten Versand („FTPS – FTP over SSL/TLS“ oder „sFTP – SSH/FTP“) zum Einsatz kommt. Für den Administrator des FTP-Servers ist dies mit wenigen Einstellungen realisierbar, die Nutzer merken dies höchstens bei der (einmaligen) Einstellung des Zugangs auf den Server für das Hochladen von Dokumenten.

Vor Nutzung der Lösung des FTP-Servers sollten die Beteiligten mit ihrer IT-Abteilung klären, ob diese Technologie genutzt werden kann: Einige Kanzleien, die sich gegen den Betrieb eines eigenen FTP-Servers entschieden haben, sperren die für FTP vorgesehenen Kommunikationskanäle (sogenannte „Ports“) aus Sicherheitsgründen standardmäßig.

³⁷ FTP mit SSH, https://de.wikipedia.org/wiki/SSH_File_Transfer_Protocol.

³⁸ IP-Adressen, <https://de.wikipedia.org/wiki/IP-Adresse>.

e) *Verwendung eines sogenannten „Datenraums“ in der Cloud*

Gegenüber der Übermittlung von Dateien als Email-Anhang oder der Verwendung des FTP-Protokolls bei großem Dateivolumen setzt sich zunehmend und zu Recht die Nutzung von Datenräumen in der sogenannten „Cloud“³⁹ durch. Dabei wird der Internetbrowser mit seiner flexiblen graphischen Benutzeroberfläche (GUI) am Arbeitsplatz als Schnittstelle zu einem auf Servern liegenden Dateiverzeichnis genutzt, das verschiedene unterstützende Funktionen bereitstellt und eine Verzeichnisdarstellung mit Ordnern, die dem gewohnten Bild am Arbeitsplatzrechner entspricht. Dateien können auf die Verzeichnisordner „gezogen“ werden oder von dort auf den Arbeitsplatz, die Übertragung erledigen die Applikationen im Hintergrund. Manche Cloud-Dienste „spiegeln“ mittels einer lokal installierten App auch gleich das ganze, in der Cloud befindliche, Verzeichnis- und Dateikonvolut auf die lokale Festplatte und halten Änderungen hierzu synchronisiert. Der Zugang zu den Verzeichnissen ist nur mit einer Nutzer-ID und einem Passwort möglich. Zudem kann und soll bei zureichendem Sicherheitsbedürfnis eine sogenannte „Multifaktoren-Authentifizierung“ (*Two Factor Authentication*/Autorisierung in zwei Schritten⁴⁰) durch Übermittlung eines zweiten Kennzeichens per SMS oder Email vorgesehen werden, was die Sicherheit des Zugangs verbessert.

Solche Datenräume können gesondert für das einzelne Schiedsverfahren eingerichtet werden. Für den einzelnen Datenraum können – jedenfalls bei der auch wegen der verfügbaren größeren Speicherraumgröße zu empfehlenden entgeltlichen Abonnementsversion – Administratorenrechte vergeben werden, vorzugsweise an den Einzelschiedsrichter oder den Vorsitzenden des Schiedsgerichts, ggf. auch an die Schiedsinstitution, wenn diese den Datenraum als Dienst vorhält. Wenn eine entgeltliche, kommerzielle Datenraumlösung für das Schiedsverfahren gewählt wird, können Zugriffsrechte verzeichnis-, ja selbst dateibezogen vom Administrator granular vergeben werden. Grundsätzlich muss ein Nutzer wenigstens ein Leserecht haben, damit er das Unterverzeichnis bzw. die Datei überhaupt am Bildschirm sieht. Zugriffsrechte auf ein übergeordnetes Verzeichnis werden grundsätzlich auf diesem untergeordneten Verzeichnis auch angewendet (vererbt), können aber nutzerbezogen auf jeder Verzeichnisebene angepasst werden. Dateien sind hier bei Leseberechtigung dauernd sichtbar und zugänglich. Das erweitert die Nutzungsmöglichkeiten. Wenn die Institution den Datenraum betreibt, wird sie regelmäßig eine für Schiedsverfahren vorkonfigurierte Verzeichnisstruktur bereitstellen und die Nutzerverwaltung organisieren. Nachfolgend wird eine Datenraumstruktur mit einem Vorschlag für die zu vergebenden Zugriffsrechte dargestellt, die für die Datenraumkonfiguration zweckmäßig, aber nicht zwingend ist. Da die GUI der Datenräume sich unterscheiden, ist diese Darstellung beispielhaft. Sie ist aber in gängigen Datenraumangeboten⁴¹ realisierbar.

³⁹ Cloud, https://de.wikipedia.org/wiki/Cloud_Computing.

⁴⁰ Zwei-Faktor-Authentifizierung, <https://de.wikipedia.org/wiki/Zwei-Faktor-Authentisierung>.

⁴¹ Beispiele: *BOX.com*, *DropBox.com* etc. *Strato HighDrive* (<https://www.strato.de/cloud-speicher/hidrive-business/>); *Uptime* (<https://www.uptime.de/>); *Luckycloud* (<https://luckycloud.de/de/>); *Brainloop* (www.brainloop.com); *Own-Cloud* (<https://owncloud.com>); *LEITZCloud* (www.leitz-cloud.com); *Tresorit* (<https://support.tresorit.com>); eine Liste mit Anbietern ist auch zu finden unter <https://www.capterra.com/de/directory/30783/virtual-data-room/software>, <https://www.capterra.com/de/directory/31310/cloud-storage/software>, etc.

Mein Bereich Erste Schritte

Download Upload Deface Rename Copy New folder Share Receive

Vorsitzender1 / Musterschiedsverfahren / Log out Vorsitzender1

Directories	Name	Last changed	Size
Vorsitzender1			
Musterschiedsverfahren			
1 Schiedsgericht	1 Schiedsgericht	2018-11-23 12:12	
2 Verfahrensstellende Verfügungen etc	2 Verfahrensstellende Verfügungen etc	2018-11-23 10:38	
3 Schiedsklägerin	3 Schiedsklägerin	2018-11-23 15:18	
4 Schiedsbeklagte	4 Schiedsbeklagte	2018-11-23 10:39	
5 Document Disclosure	5 Document Disclosure	2018-11-23 15:21	
6 Dokumente für Schiedsverhandlung	6 Dokumente für Schiedsverhandlung	2018-11-23 15:29	

Share links (0)
Receive points (0)

Powered by dTPServer © Vastigata-Data AG

Benutzername: Vorsitzender1
 Passwort: *****
 Display name: Vorsitzender1
 Mitglied von: [Dropdown]

Allow login
 Passwort benötigt
 Administratorzugang

Stammverzeichnis | Einschränkungen | Sicherheit | Services | Ereignisse und Meldungen | Statistiken

Files	Directories	Permissions
Musterschiedsverfahren		
1 Schiedsgericht	C:\Datarooms\Musterschiedsverfahren\1 Schiedsgericht	<input checked="" type="checkbox"/>
2 Verfahrensstellende Verfügungen etc	C:\Datarooms\Musterschiedsverfahren\2 Verfahrensstellende Verfügungen etc	<input checked="" type="checkbox"/>
3 Schiedsklägerin	C:\Datarooms\Musterschiedsverfahren\3 Schiedsklägerin	<input checked="" type="checkbox"/>
4 Schiedsbeklagte	C:\Datarooms\Musterschiedsverfahren\4 Schiedsbeklagte	<input checked="" type="checkbox"/>
5 Document Disclosure	C:\Datarooms\Musterschiedsverfahren\5 Document Disclosure	<input checked="" type="checkbox"/>
6 Dokumente für Schiedsverhandlung	C:\Datarooms\Musterschiedsverfahren\6 Dokumente für Schiedsverhandlung	<input checked="" type="checkbox"/>
	C:\Datarooms\Musterschiedsverfahren	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/>

Dateien
 Lesen
 Schreiben
 Löschen
 Anhängen

Verzeichnisse
 Auflisten
 Erstellen
 Löschen
 +Unterverz.

Verschiedenes
 Versteckte ignorieren
 Speicherpl. begr.
 0 MB

Benutzername: Schiedsrichter2
 Passwort: *****
 Display name: Schiedsrichter2
 Mitglied von: [Dropdown]

Allow login
 Passwort benötigt
 Administratorzugang

Stammverzeichnis | Einschränkungen | Sicherheit | Services | Ereignisse und Meldungen | Statistiken

Files	Directories	Permissions
Musterschiedsverfahren		
1 Schiedsgericht	C:\Datarooms\Musterschiedsverfahren\1 Schiedsgericht	<input checked="" type="checkbox"/>
2 Verfahrensstellende Verfügungen etc	C:\Datarooms\Musterschiedsverfahren\2 Verfahrensstellende Verfügungen etc	<input checked="" type="checkbox"/>
3 Schiedsklägerin	C:\Datarooms\Musterschiedsverfahren\3 Schiedsklägerin	<input checked="" type="checkbox"/>
4 Schiedsbeklagte	C:\Datarooms\Musterschiedsverfahren\4 Schiedsbeklagte	<input checked="" type="checkbox"/>
5 Document Disclosure	C:\Datarooms\Musterschiedsverfahren\5 Document Disclosure	<input checked="" type="checkbox"/>
6 Dokumente für Schiedsverhandlung	C:\Datarooms\Musterschiedsverfahren\6 Dokumente für Schiedsverhandlung	<input checked="" type="checkbox"/>
	C:\Datarooms\Musterschiedsverfahren	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/>

Dateien
 Lesen
 Schreiben
 Löschen
 Anhängen

Verzeichnisse
 Auflisten
 Erstellen
 Löschen
 +Unterverz.

Verschiedenes
 Versteckte ignorieren
 Speicherpl. begr.
 0 MB

Benutzername: Schiedsrichter3
 Passwort: *****
 Display name: Schiedsrichter3
 Mitglied von: [Dropdown]

Allow login
 Passwort benötigt
 Administratorzugang

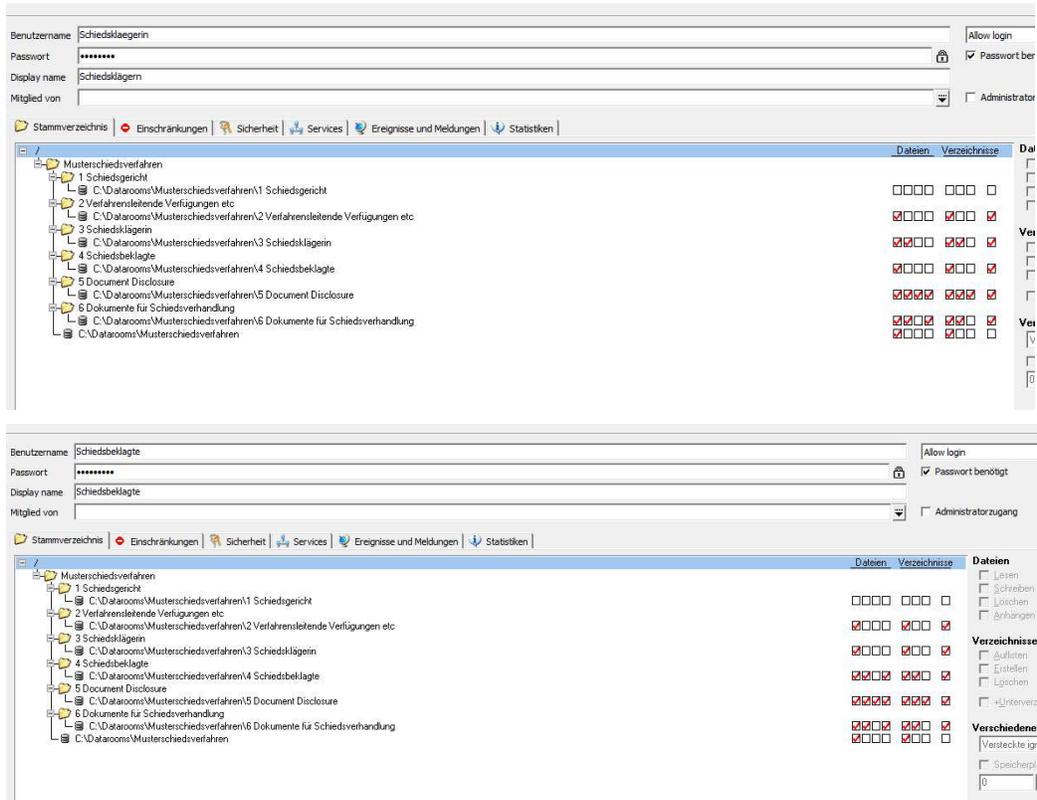
Stammverzeichnis | Einschränkungen | Sicherheit | Services | Ereignisse und Meldungen | Statistiken

Files	Directories	Permissions
Musterschiedsverfahren		
1 Schiedsgericht	C:\Datarooms\Musterschiedsverfahren\1 Schiedsgericht	<input checked="" type="checkbox"/>
2 Verfahrensstellende Verfügungen etc	C:\Datarooms\Musterschiedsverfahren\2 Verfahrensstellende Verfügungen etc	<input checked="" type="checkbox"/>
3 Schiedsklägerin	C:\Datarooms\Musterschiedsverfahren\3 Schiedsklägerin	<input checked="" type="checkbox"/>
4 Schiedsbeklagte	C:\Datarooms\Musterschiedsverfahren\4 Schiedsbeklagte	<input checked="" type="checkbox"/>
5 Document Disclosure	C:\Datarooms\Musterschiedsverfahren\5 Document Disclosure	<input checked="" type="checkbox"/>
6 Dokumente für Schiedsverhandlung	C:\Datarooms\Musterschiedsverfahren\6 Dokumente für Schiedsverhandlung	<input checked="" type="checkbox"/>
	C:\Datarooms\Musterschiedsverfahren	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/>

Dateien
 Lesen
 Schreiben
 Löschen
 Anhängen

Verzeichnisse
 Auflisten
 Erstellen
 Löschen
 +Unterverz.

Verschiedenes
 Versteckte ignorieren
 Speicherpl. begr.
 0 MB



Nachfolgend zeigen wir tabellarisch die Konfiguration der Zugriffsberechtigungen der einzelnen Verzeichnisse, wobei die höchste Verzeichnisebene das Verzeichnis „Musterschiedsverfahren“ ist (Vorsitzender ist hier funktional gleich Alleinschiedsrichter).

0 Musterschiedsverfahren				
		Lesen	Schreiben	Löschen
(1)	Vorsitzender	x	x	x
(2)	Mitschiedsrichter 1 + 2	x	x	
(3)	Schiedskläger	x		
(4)	Schiedsbeklagte	x		

1 Schiedsgericht				
		Lesen	Schreiben	Löschen
(1)	Vorsitzender	x	x	x
(2)	Mitschiedsrichter 1 + 2	x	x	

2 Verfahrensleitende Anordnungen etc.				
		Lesen	Schreiben	Löschen
(1)	Vorsitzender	x	x	x
(2)	Mitschiedsrichter 1 + 2	x		

(3)	Schiedskläger	x		
(4)	Schiedsbeklagte	x		

3 Schiedskläger				
		Lesen	Schreiben	Löschen
(1)	Vorsitzender	x		x
(2)	Mitschiedsrichter 1 + 2	x		
(3)	Schiedskläger	x	x	
(4)	Schiedsbeklagte	x		

4 Schiedsbeklagte				
		Lesen	Schreiben	Löschen
(1)	Vorsitzender	x		x
(2)	Mitschiedsrichter 1 + 2	x		
(3)	Schiedskläger	x		
(4)	Schiedsbeklagte	x	x	

5 Document Disclosure – Parteiintern)				
		Lesen	Schreiben	Löschen
(1)	Vorsitzender	?		x
(2)	Mitschiedsrichter 1 + 2			
(3)	Schiedskläger	x	x	x
(4)	Schiedsbeklagte	x	x	x

6 Dokumente für Schiedsverhandlung				
		Lesen	Schreiben	Löschen
(1)	Vorsitzender	x	x	x
(2)	Mitschiedsrichter 1 + 2	x		
(3)	Schiedskläger	x	x	
(4)	Schiedsbeklagte	x	x	

Innerhalb der Unterverzeichnisse „Schiedskläger“ und „Schiedsbeklagte“ können diese weitere Unterverzeichnisse anlegen, wie das oben für ZIP-Archive aufgezeigt wurde. Die Berechtigungen sind jeweils identisch mit jenen des direkt übergeordneten Verzeichnisses, solange keine besondere Konfiguration der Rechte für dieses Verzeichnis erfolgt ist.

Das Verzeichnis „*Document Disclosure*“ mit seinen Inhalten soll nur für die Parteien lesbar sein. Allerdings werden möglicherweise für Einzelschiedsrichter oder Vorsitzende gewisse Administratorrechte vorgesehen werden müssen. Alternativ lässt sich im Datenraum ein besonderes Verzeichnis anlegen, das als Nutzergruppe ausschließlich den Parteien zugewiesen ist.

Das Verzeichnis „Dokumente für Schiedsverhandlung“ erlaubt die Zusammenstellung einer auf die Bedürfnisse der mündlichen Verhandlung zugeschnittenen Dokumentation, die aus den Ordnern „Schiedskläger“ und „Schiedsbeklagte“ herüberkopiert oder mit diesen durch Hyperlinks verknüpft werden. Dazu im folgenden Abschnitt II.5.

Solche virtuellen Datenräume sind nach Einrichtung von allen Beteiligten leicht nutzbar und halten die gesamte Schiedsakte, in dem je nach Rolle im Verfahren erforderlichen Umfang an einem „logischen“ Ort verfügbar, so dass stets Transparenz des Status der Akteninhalte (der Dateien) gewährleistet ist. Aufgrund seiner Berechtigungen hat zumindest das Schiedsgericht auch durch den Vorsitzenden bzw. Einzelschiedsrichter eine Transparenz hinsichtlich der Zugriffe, wenn dieses Thema relevant sein sollte. Die eingesetzten technischen Verfahren sind, mit Ausnahme der anfänglichen Konfiguration, allen Verfahrensbeteiligten von ihren Arbeitsplatzrechnern bekannt oder einfach zu erlernen. Wenn Dateien nicht irgendwie auch in größerer Zahl gemeinsam in den Datenraum hoch- und heruntergeladen werden können, wird die Arbeit auch hier durch die Nutzung von „Containern“ (zB ZIP-Dateiarchiven) erleichtert.

Auch hier sind jedoch Sicherheits- und Datenschutzaspekte bei der Auswahl des den Datenraum anbietenden Betreibers geboten, da dieser übergeordnete Administratorrechte hat, die selbst für das Schiedsgericht regelmäßig nicht transparent sind. Das gilt selbst dann, wenn die Daten im Datenraum betreiberseitig verschlüsselt gespeichert werden. Die AGB der Betreiber geben diesen zudem oft „überschießende“ Rechte, insbesondere Zugriffs- und Weitergaberechte, was zu beachten ist. Dem Geheimnisschutz und dem allgemeinen Schutz vor der Kenntnisnahme durch Dritte im Fall des unerwünschten Zugriffs auf die Server des Dienstanbieters sollte hier deshalb durch die Wahl einer sogenannten „*Zero-Knowledge*“-Lösung Rechnung getragen werden, bei der die Daten durch eine Ende-zu-Ende-Verschlüsselung bereits vor dem Hochladen in die Cloud so verschlüsselt werden, dass auch der Administrator/Betreiber die Daten nicht entschlüsseln kann.⁴² Datenschutzrechtlich ist auf eine physische Lokalisierung der genutzten Serverhardware in der EU und/oder wenigstens eine Zertifizierung des Dienstes auf DGSVO-Konformität zu achten.⁴³ Bei Dienstleistern insbesondere außerhalb der EU, insbesondere bei Anbietern mit Sitz auch in den USA ist zudem ggf. auf staatliche Zugriffsrechte zu achten.⁴⁴ Zu klären ist weiter, dass und wann die Daten nach Verfahrensende vollständig (Back-Up!⁴⁵) gelöscht werden.

Für große Schiedsverfahren, bei denen der (Kosten-)Aufwand sich lohnt, bieten sich auch integrierte Plattformen an, die neben der Funktion „Datenraum“ eine Digitalisierung der mündlichen Verhandlung einschließlich deren Aufzeichnung und Transkription sowie die Einbindung von interner Unterstützung der Vertreterteams aus der Ferne anbieten.⁴⁶

⁴² Vgl. zu 0-Knowledge zB <https://de.wikipedia.org/wiki/Zero-Knowledge-Beweis>; <https://tresorit.com/blog/zero-knowledge-verschlüsselung/>, <https://www.cloudwards.net/best-zero-knowledge-cloud-services/>, <https://www.boxcryptor.com/de/blog/post/zero-knowledge-cloud-security/>.

⁴³ Vgl. zB Angebote von zB *Strato HighDrive* (<https://www.strato.de/cloud-speicher/hidrive-business/>); *Uptime* (<https://www.uptime.de/>); *Luckycloud* (<https://luckycloud.de/de/>); *Brainloop* (www.brainloop.com); *OwnCloud* (<https://owncloud.com>); *LEITZCloud* (www.leitz-cloud.com); *Tresorit* (<https://support.tresorit.com>) etc.

⁴⁴ In den USA der *CLOUD Act*, https://de.wikipedia.org/wiki/CLOUD_Act.

⁴⁵ *Back Up* – Datensicherung, <https://de.wikipedia.org/wiki/Datensicherung>.

⁴⁶ Als Beispiel sei hier *Opus2™* (<https://www.opus2.com/>) genannt.

Solange die so referenzierte Datei nicht in der Verzeichnisstruktur verschoben oder gelöscht wird, öffnet sie sich durch Anklicken des Hyperlinks in der Tabelle. Mit der Sortierfunktion der Programme ist es dann zB je nach aktuellem Bedarf leicht möglich, nach Eingabe von deren historischem Datum eine chronologische Gliederung oder eine Gliederung nach Verfassernamen usw. in der Tabelle variabel vorzunehmen.

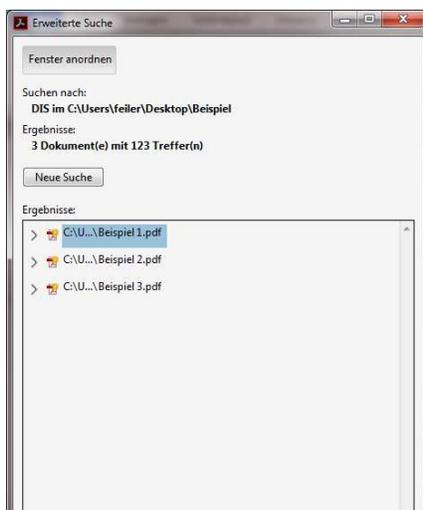
Zudem kann man (wie oben beschrieben), wenn das nicht schon der Fall ist, mit den entgeltlichen Programmen zur PDF-Dateianzeige und Verarbeitung den Text der PDF-Dateien erkennen (OCR – siehe oben II.3.c), so dass er über die Volltextsuche im System des Arbeitsplatzrechners oder mit speziellen Programmen durchsuchbar ist.

Liegen mehrere PDF-Dokumente mit OCR vor, kann auch übergreifend in mehreren Dokumenten gesucht werden:

Im Beispiel wird das kostenlose Programm *Adobe Acrobat Reader DC* verwendet. Über „Bearbeiten“ -> „Erweiterte Suche“ wird der oa Suchdialog aufgerufen und anschließend auf ein Verzeichnis mit mehreren PDF-Dateien gelenkt. In diesem Verzeichnis wird dann nach dem Schlüsselwort „DIS“ gesucht.



Das Ergebnis wird – gruppiert nach Dokumenten – angezeigt:



Für die Arbeit des Schiedsgerichts an eigenen Entwürfen ist die Ein-Text-Methode gut geeignet, bei der ein erster Entwurf im „Änderungen-nachverfolgen“-Modus bearbeitet wird, der jede Modifikation hervorhebt und Kommentare im Text an jeder Stelle ermöglicht. Damit die Stadien des einen Textes nachvollziehbar bleiben, hat es sich bewährt, den Dateinamen mit dem Kürzel des

letzten Bearbeiters zu ergänzen und dem Datum. So ist leicht zu sehen, mit welcher Version man arbeitet.

Für all dies ist grundsätzlich unerheblich, ob die Arbeit direkt im Datenraum in der Cloud im dafür bestimmten Verzeichnis erfolgt oder auf dem eigenen Arbeitsplatzrechner mit nachfolgender Übertragung der Datei an die Empfänger.

Wenn ein Datenraum genutzt wird und die Parteien ein Dokument gemeinsam mitbearbeiten, wie das zB bei *Redfern Schedules* der Fall ist, ist es besser, wenn sie eine einzige Datei im virtuellen Datenraum dazu bearbeiten, anstatt diese zu zirkulieren.

Findet sich in der Akte ein Dokument in eine Sprache, die nicht Verfahrenssprache ist und die der Leser nicht versteht, kann mit Übersetzungsprogrammen oder Werkzeugen in der Cloud ausschließlich zur *prima facie* inhaltlichen Relevanzprüfung – nicht als Grundlage für die juristische Auslegung – eine Maschineübersetzung angefertigt werden. Diese AI-Technik schreitet wie die Spracherkennung schnell voran. Jedoch stellen sich bei kostenlosen Diensten auch hier Probleme der Vertraulichkeit und des Datenschutzes, weil unkontrolliert ein Drittzugriff auf die Daten stets möglich ist. Es kann aber auf Bezahldienste⁵¹ zurückgegriffen werden.

6. Video- und Audiokonferenzen

a) Audiokonferenzen

Audiokonferenzen werden heute, aufgrund der Digitalisierung der Telefonienetzwerke und den damit anbieterbaren Konferenzschaltungsangeboten, von einer Vielzahl von Anbietern in der Wirtschaft zur Verfügung gestellt und von Anwälten intensiv verwendet und bereiten keine Probleme bei der Nutzung im Zusammenhang mit Schiedsverfahren. Problemlos werden sie bei internen Beratungen des Schiedsgerichts oder zur Absprache von Organisations- bzw. Verfahrensfragen, zB bei der ersten Besprechung des Schiedsgerichts mit den Parteien, eingesetzt. Dazu sucht man einen Dienstleister, generiert bei diesem einen Code für den virtuellen Besprechungsraum sowie ggf. eine Nutzer-ID und verteilt diese Informationen in geeigneter Weise (meist per Email, elektronisch im Email-Client generierte Besprechungseinladung, etc.) mit der Einwahlzeit an die Teilnehmer. Diese wählen sich dann ein und zu Beginn wird die „Anwesenheit“ festgestellt.

Allerdings wird gelegentlich die Kommunikationsqualität gestört, weshalb hier einige ganz praktische und banale Dinge zu berücksichtigen sind:

a) Es sollte möglichst eine professionelle Freisprecheinrichtung oder ein Head-Set (Kopfhörer-Mikrofon-Kombination) benutzt werden, schon um die Hände frei zu haben, aber auch wegen der Tonqualität.

b) Jeder Teilnehmer sollte sich in einem Raum befinden, der von Störgeräuschen (Straßenlärm usw.) frei ist und, wenn sie/er nicht einen Wortbeitrag leistet, auf stumm (mute) schalten. Akten, in denen während der Telefonkonferenz geblättert wird, sollten nicht direkt vor dem Mikrofon liegen. Gleiches gilt für PC-Tastaturen.

Vorteil der Nutzung von Audiokonferenzen ist, dass sie An- und Abreisezeiten und den mit einer Reise verbundenen weiteren Aufwand entfallen lassen. Zudem ist es regelmäßig leichter, unter den vielen Beteiligten einen verfügbaren Termin zu finden, weil das benötigte Zeitfenster kleiner ist und der Einwahlort im Grundsatz keinen weiteren Beschränkungen unterliegt.

b) Videokonferenzen

⁵¹ Bspw. *Deep L Pro* (www.deepl.com) oder *Systran* (<http://www.systran.de>).

Videokonferenzen⁵² finden über das Internet mit IP-Kommunikation⁵³ statt und setzen einen Breitbandzugang bei allen Beteiligten voraus. Das ist heute regelmäßig, aber bei weitem nicht immer der Fall. Sie haben die gleichen Vorteile wie Audiokonferenzen. Gegenüber Audiokonferenzen haben Videokonferenzen zwei zusätzliche Vorteile. Weil man den Sprecher sieht, kann man die Beiträge einfacher zuordnen, als dies der Fall ist, wenn man an die Stimmen der Teilnehmer noch nicht gewöhnt ist. Videokonferenzsysteme verfügen häufig über Zusatzfunktionen, die es erlauben, Dokumente anzuzeigen, auf die im Gespräch Bezug genommen wird. Psychologisch vermitteln Videokonferenzen den Eindruck größerer Unmittelbarkeit.

Videokonferenzen können mit speziellen Videokonferenzsystemen durchgeführt werden, wenn alle Beteiligten über ein kompatibles System bestehend aus der Hardware mit Kamera, Bildschirm oder Projektor und Sprachsystem (Lautsprecher, Konferenzmikrofon) sowie der Videokonferenz-einheit verfügen, die regelmäßig in einem besonderen Konferenzraum installiert sind. Sie müssen von geschultem Personal technisch vorbereitet werden, da das Verfahren zur Verbindung via IP technisch anspruchsvoller ist als die Einwahl per Telefon. Wenn nicht die identischen Teilnehmer schon erfolgreich eine Videokonferenz abgehalten haben, sollte rechtzeitig vor der Konferenz ein technischer Funktionstest (Verbindungstest) durchgeführt werden. Es gelten auch hier die Empfehlungen zur Sicherstellung der Tonqualität. Zusätzlich ist darauf zu achten, dass sich hinter den Teilnehmern keine Lichtquelle befindet. Bild- und Tonqualität sind, wenn die technischen Anforderungen erfüllt sind, so hoch, dass solche Systeme beim Einsatz in der mündlichen Verhandlung (siehe unten II.7.b) anderen Lösungen in der Kommunikationsqualität überlegen sind.

Videokonferenzen können heute auch am Arbeitsplatzrechner durchgeführt werden, wenn dort ein Breitbandanschluss, eine sogenannte WebCam,⁵⁴ ein Mikrofon und ein Lautsprecher bzw. ein Kopfhörer mit Mikrofon verfügbar sind, sowie der entsprechende Videokonferenzclient⁵⁵ installiert ist. Organisation der Konferenz und Verbindungsherstellung sind einfach zu erlernen. Diese technische Lösung ist jedenfalls immer dann gut geeignet, wenn sie funktional an Stelle einer Audiokonferenz tritt. Für diese Videokonferenzen gelten die gleichen Empfehlungen wie für jene mit dediziertem Videokonferenzsystem. Jedoch erübrigt sich meist ein Test durch Fachpersonal. Zu beachten ist jedoch, dass jeder Anbieter von Videokonferenzclients dafür eine eigene Infrastruktur betreibt, die grundsätzlich nicht mit den Systemen anderer Anbieter interoperabel ist. Alle Beteiligten müssen also den Client⁵⁶ des gleichen Anbieters nutzen. Konferenzteilnehmer, deren Arbeitsplatz in das Netzwerk einer Organisation eingebunden ist und die den Client zuvor nicht genutzt haben, müssen mit dem bei ihnen zuständigen Netzwerkadministrator nicht nur rechtzeitig sicherstellen, dass sie dieses Programm installieren können (dürfen), sondern auch, dass die für den Client nötigen Kommunikationsprotokolle im Netzwerk unterstützt und nicht von der Firewall⁵⁷ blockiert werden.

Auch für Audio- und Videokonferenzen gilt, dass der zu nutzende Dienst auf seine Sicherheit und Vertrauenswürdigkeit sowie ggf. auf Einhaltung der DSGVO zu prüfen ist. Zudem ist ggf. auf staatliche Zugriffsrechte zu achten.

⁵² Videokonferenz, <https://de.wikipedia.org/wiki/Videokonferenz>.

⁵³ IP-Kommunikation, <https://de.wikipedia.org/wiki/IP-Telefonie>.

⁵⁴ WebCam, <https://de.wikipedia.org/wiki/Webcam>.

⁵⁵ Videoprogramme wie zB *Skype*, *Zoom*-, *GoToMeeting*, *Cisco WebEx*, etc., https://de.wikipedia.org/wiki/Liste_von_Webkonferenz-Lösungen, www.gotomeeting.com; *Adobe Connect*, www.adobe.com/de/products/adobeconnect/meetings.html, s. auch für eine Anbieterübersicht <https://www.capterra.com/de/directory/30075/web-conferencing/software>.

⁵⁶ Client, <https://de.wikipedia.org/wiki/Client>.

⁵⁷ S. <https://de.wikipedia.org/wiki/Firewall>

7. Mündliche Verhandlung

Technologisch ist es möglich, auf die Nutzung von körperlichen Akten in der mündlichen Verhandlung zu verzichten, wenn die Beteiligten damit aufgrund ihrer Arbeitspraxis zurechtkommen. Dadurch wird jedenfalls der Transportaufwand reduziert. Erforderlich sind dazu für jeden Verfahrensbeteiligten ein Rechner mit Bildschirm (zB ein Laptop) und ein Hochgeschwindigkeitsnetzwerkzugang sowie vorzugsweise ein einziger Projektor oder montierter Projektionsbildschirm, der für den Vortrag wesentliche Dokumente für alle anzeigt oder auch Präsentationen. Dokumente können anwesenden Zeugen auf einem speziell für sie aufgestellten Bildschirm vorgehalten werden.

a) *Präsentation von Beweisurkunden etc.*

Ein virtueller Datenraum (siehe oben II.4.e), in dem ein Verzeichnis für die in der Verhandlung wesentlichen Dokumente (Dateien) mit einer Inhaltsverzeichnisdatei, die auf diese per Hyperlink verweist, liegt und auf den alle Beteiligten während der Verhandlung über den Browser ihres Rechners zugreifen, kann die Verhandlungsvorbereitung und die Nutzung der Dokumente während der Verhandlung gegenüber einem Aufruf nur am eigenen Rechner vereinfachen. Hierzu eingesetzt werden können auch Programme zur Teilung von Bildschirmhalten über Netzwerke.⁵⁸ Ein vom Vortragenden aufgerufenes Dokument ist so für alle weiteren Verfahrensbeteiligten direkt, ohne eigenes Suchen, anzeigbar. Das ist ein Vorteil gegenüber konventionellen Akten.

Möglich, aber weniger komfortabel ist es, dass der Vortragende die Dokumente an seinem Rechner aufruft und per Projektor für alle anderen Beteiligten sichtbar macht.

b) *Videokonferenzen*

Videokonferenzen können auch während der Verhandlung genutzt werden.

aa) *Zeugen- und Sachverständigenbefragungen*

Obwohl die Zeugen- oder Sachverständigenbefragung mit einem dedizierten Videokonferenzsystem aufgrund ihrer technischen Qualität vorzuziehen ist, können Zeugen auch mit den am Arbeitsplatzrechner installierten Videokonferenzclients angehört werden. Weil die menschliche Wahrnehmung bei persönlicher Anwesenheit mehr Kommunikationskanäle nutzen kann und vielfältiger ist, wird bei einer Zeugenanhörung über Videokonferenzschaltung eine gewisse Reduzierung der Kommunikationsqualität eintreten. Deshalb sollte abgewogen werden, ob dieser Nachteil dadurch kompensiert wird, dass zB der Zeuge anderenfalls am Verhandlungstag gar nicht verfügbar wäre oder der Aufwand seiner An- und Abreise unangemessen hoch ist.

Für den technischen Rahmen dieser Anhörung gilt das oben allgemein zu Videokonferenzen Ausgeführte. Hier ist lediglich zusätzlich zu prüfen, ob ein erhebliches Risiko darin gesehen wird, dass der Zeuge zwar im Sichtfeld der WebCam zu sehen ist, aber nicht der Rest seines Umfelds; hier also Beeinflussungsmöglichkeiten bestehen, die bei körperlicher Anwesenheit des Zeugen in der Verhandlung nicht vorlägen. Eine einfache Vorkehrung ist hier dann die Entsendung von Hilfspersonal jeder Partei zur Überwachung an den Ort, wo der Zeuge körperlich sitzt.

bb) *Mündliche Verhandlung per Videokonferenz*

So wie die Parteien auf eine mündliche Verhandlung verzichten können, sind sie in Übereinstimmung mit dem Schiedsgericht nicht gehindert, die beschriebenen Videokonferenztechnologien zur Durchführung der gesamten mündlichen Verhandlung zu nutzen, was regelmäßig auch den Ein-

⁵⁸ Bspw. *TeamViewer*TM, <https://de.wikipedia.org/wiki/TeamViewer>, Präsentationsfunktionen enthalten auch die meisten, im Text unter II.4.b, für Arbeitsplatzrechner genannten Lösungen; für Liste von *Screen-Sharing*-Lösungen s. <https://de.wikipedia.org/wiki/Screen-Sharing>.

satz der erwähnten *Screen-Sharing*-Programme erfordert. Voraussetzung ist freilich ein sicheres Beherrschen der Bedienung der Programme. Entscheidend ist hier weniger die Technik, sondern vielmehr die legitimen Erwartungen der Parteien an das Verfahren. Längere Verhandlungen kommen hier wohl bei Berücksichtigung des Faktors Mensch nicht in Betracht. Geeignet erscheinen Eilsachen und im Umfang kleinere Fälle. Im Jahr 2018 fehlten praktische Erfahrungen.

cc) *Zuschaltung von Dienstleistern wie Dolmetschern*

Es kann erforderlich sein, Dolmetscher, Simultanübersetzer oder Stenographen bei der Verhandlung einzusetzen, deren Anreise und Unterbringungskosten eingespart werden können, wenn sie per Audiokonferenz zugeschaltet werden. Derartige Dienstleistungen werden allerdings vornehmlich von Anbietern in den USA und nicht im deutschen Inland angeboten. Da die technischen Voraussetzungen aber jenen entsprechen, die für Konferenzschaltungen im Allgemeinen gelten, ist bei sorgfältiger Vorbereitung auch hier zumindest die Kosteneffizienz steigerbar. Hier gelten für die Zuschaltungsprogramme ebenfalls die zu Webdiensten wie Datenräumen oder Videokonferenzen oben angestellten Sicherheitsüberlegungen. Zudem ist dem Datenschutzrecht durch eine geeignete Vereinbarung Rechnung zu tragen (siehe unten II.9.c).

c) *Aufzeichnung der Verhandlung*

Die Effizienz eines in „deutscher Manier“ vom Vorsitzenden/Einzelschiedsrichter unmittelbar diktierten und später übermittelten Sitzungsprotokolls wird von technischen Lösungen schwerlich überboten. Jedoch ist sie in komplexen Angelegenheiten, in denen viele Zeugen angehört werden, weniger geeignet und auch international unüblich. Dort können, soweit eine sofortige Verfügbarkeit des Wortmittschnitts gewünscht ist, Gerichtsstenographen (*court reporter*) mit Softwarelösungen kombiniert werden, welche die Mitschrift sofort am Bildschirm und ausdrückbar quasi zeitgleich den Verfahrensbeteiligten bereitstellen.⁵⁹ Weil die Kosten der Gerichtsstenographen und der Miete des Echtzeittranskriptionssystems erheblich sind, bleiben sie großen Verfahren vorbehalten. Mit den spracherkennungs-basierten Lösungen liegen 2018 noch keine Erfahrungen zur Ausgereiftheit vor.

Die verfügbare technisch stabile Lösung besteht deshalb im digitalen Audiomittschnitt der Verhandlung mit einem Aufzeichnungsprogramm, welches das Setzen von digitalen Marken (zB „Beginn Zeugnis n.n.“) in der Aufzeichnung erlaubt. Der Mittschnitt wird danach zumindest in seinen wesentlichen Teilen händig getippt und als Wortmitschrift verteilt. Zur Aufzeichnung gibt es Konferenzsysteme.⁶⁰ Technisch benötigt werden eine für alle Sprecher ausreichende Zahl von Aufzeichnungsmikrofonen, die entweder miteinander verbunden werden können oder die über ein kleines Mischpult mit ausreichenden Eingängen an einen dedizierten Audiorecorder⁶¹ oder einen Computer mit einem geeigneten Aufzeichnungsprogramm⁶² angeschlossen werden. Eine Hilfskraft sollte den Recorder während der Verhandlung bedienen.

Solange kein zuverlässiges Spracherkennungsprogramm den Mittschnitt automatisch in Text umwandelt, wird der Aufwand dadurch deutlich reduziert, dass auf eine Transkription des gesamten Mittschnitts verzichtet und er als Audiodatei verteilt wird. Vorausgesetzt, die digitalen „Marker“ wurden korrekt gesetzt, sind Aussageteile gleichwohl gut in der Aufzeichnung zu finden. Bei Be-

⁵⁹ Bspw. *CaseView*, <http://www.stenograph.com/caseviewnet-information>; *LiveNote*, <https://legal.thomsonreuters.com/en/products/livenote-stream>). Allerdings werden derzeit auch erste Lösungen angeboten, die mit Spracherkennung automatisch transkribieren (zB <https://www.amberscript.com/de>; *SONIX*, <https://sonix.ai/>; *Voicebase*, <https://www.voicebase.com/speech-to-text/>).

⁶⁰ Bspw. jene von *Beyer* oder *Philips*, www.beyerdynamic.de/konferenztechnik.html, www.philips.de/c-p/LFH0955_10/.

⁶¹ Bspw. die Recorder von *Tascam*, www.tascam.eu uvm.

⁶² Bspw. *Audacity*, s. www.audacity.org

darf werden dann nur wesentliche Aussageteile transkribiert. Ob dieses Einsparungspotenzial genutzt wird, hängt ausschließlich an der Arbeitsgewohnheiten der Verfahrensbeteiligten.

d) *Terminfindung*

Die Abstimmung verfügbarer Termine im Schiedsgericht oder mit den Parteien ist nicht immer einfach. Im Geschäftsleben bewährt haben sich Werkzeuge zur Terminabstimmung in der Cloud.⁶³

8. Zusammenarbeit im Schiedsgericht

a) *Konferenzschaltungen zur Beratung*

Audio- und Videokonferenzschaltungen sind in jedem Stadium ein geeignetes und effizientes Mittel zur Abstimmung unter Schiedsrichtern. Für persönliche Treffen muss ein besonderer Grund vorliegen oder sie müssen sich sonst anbieten, zB aus Anlass der mündlichen Verhandlung.

b) *Arbeit an Entwürfen*

Vielfach werden Entwürfe im Schiedsgericht per Email zirkuliert und die Kommentare dazu werden in getrennten individuellen Nachrichten übermittelt. Bei der Bearbeitung einer Dateiversion kann jedoch viel effizienter unter Verwendung der „Änderungen-nachverfolgen“- und „Kommentar“-Funktionen gearbeitet werden, die alle gängigen Textverarbeitungsprogramme bereithalten. Bei Verwendung des virtuellen Datenraums kann an einer einzigen Datei gearbeitet werden. Weil alles in einem Text zusammengefasst ist, kann dieser zügiger abgestimmt und fertiggestellt werden, als das bei einem Abgleich verschiedener Texte möglich wäre. Es gibt für die Dokumentenzusammenarbeit auch spezielle Werkzeuge in der Cloud.⁶⁴

9. Daten- und Systemsicherheit

Daten und Systemsicherheit spielen auch in der Schiedsgerichtsbarkeit eine zunehmende Rolle⁶⁵ in der Wahrnehmung. Praktische Konsequenzen werden daraus selten gezogen. Wir empfehlen, dass Parteien und Schiedsgericht zu Verfahrensbeginn eine Gefahrenabschätzung vornehmen, bei der Notwendigkeiten der Geheimhaltung und der Compliance zB mit der DGSVO und der Bedeutung des Falls dem erwarteten Bedrohungsrisiko gegenübergestellt werden. Das Niveau der zu ergreifenden Schutzmaßnahmen wird sich an dieser Bewertung orientieren.

a) *Allgemeine Systemsicherheit bei den Verfahrensbeteiligten*

Es wird unterstellt, dass Parteien aus Industrie und größerem Gewerbe ebenso wie Anwaltskanzleien über Datenverarbeitungssysteme verfügen, die dem Stand der Technik entsprechend gegen Bedrohungen gesichert sind. Einen Überblick über geeignete und erforderliche Maßnahmen gibt die Webseite des Bundesamts für Sicherheit in der Informationstechnik (BSI).⁶⁶

Wenn Verfahrensbeteiligte nicht über eine solche Sicherheitsarchitektur verfügen, wie zB allein tätige Schiedsrichter, sind sie technisch gesehen das schwächste Glied der Sicherheitsprozesse. Sie

⁶³ Bspw. das beliebte aber datenschutzrechtlich wohl auch problematischere „Doodle“ (<https://doodle.com/de/>). Sicherer sind Duddle.inf (duddle.inf.tu-dresden.de/) oder der DFN-Terminplaner (www.dfn.de/dienstleistungen/dfnterminplaner).

⁶⁴ Bspw. *SmashDocs*, www.smashdocs.net.

⁶⁵ S. zB das *ICCA Project* <https://www.arbitration-icca.org/projects/Cybersecurity-in-International-Arbitration.html>.

⁶⁶ BSI, www.bsi.bund.de, dort insbesondere

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Leitfaden_zur_Basis-Absicherung.pdf?jsessionid=AA1CDDC1BF92A201801BA87E30C876EC.1_cid351?__blob=publicationFile&v=3

und https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Download/FD_BS_Kompendium.pdf?__blob=publicationFile&v=6.

sind auch mit den technischen Erfordernissen des Sicherheitsmanagements überfordert. Gleichwohl können und müssen sie ein Mindestmaß an Sicherheit für ihre Datenverarbeitung und Kommunikation gewährleisten.

Die Maßnahmen hierzu sind, bei angenommener Nutzung eines Arbeitsplatzrechners und eines WLAN⁶⁷ im Wesentlichen folgende:

- (a) Der Rechner wird nur beruflich genutzt und nicht von Dritten. Er ist durch ein zureichend komplexes Passwort geschützt, das nur für den Zugang zu diesem Gerät, dh nicht überall, zB beim Einkauf im Internet, verwendet wird.
- (b) Das Betriebssystem des Rechners und die auf ihm installierten Programme werden laufend aktualisiert.
- (c) Die Festplatte ist verschlüsselt.⁶⁸ Zumindest sind die Verzeichnisse mit den Dateien des Verfahrens verschlüsselt und kennwortgeschützt.
- (d) Die Arbeit auf dem Arbeitsplatzrechner findet nicht in einem Konto mit Administratorrechten statt, sondern in einem einfachen Nutzerkonto ohne Berechtigung zur Programminstallation.
- (e) Insbesondere Webbrowser werden so konfiguriert, dass sich auf ihnen ausführbarer Code nicht „einnisten“ kann.
- (f) Es werden nur für die Arbeit benötigte Programme installiert, deren Quelle man vertrauen darf. Sie erhalten nur die Rechte, die sie für ihre Funktion dringend benötigen.
- (g) Auf dem Arbeitsplatzrechner läuft ein ständig aktualisiertes Virenschutzprogramm.
- (h) Auf dem Arbeitsplatzrechner läuft eine Personal Firewall mit hoher Schutzstufe.
- (i) Verbindungen zu einem WiFi⁶⁹ LAN sind verschlüsselt und passwortgeschützt. Geräte müssen anhand ihrer Kennung ausdrücklich zum Netzwerk zugelassen werden.
- (j) Jedenfalls die mobilen Geräte sind über Steuersoftware bei Verlust aus der Ferne zu löschen

Diese Maßnahmen gelten entsprechend auch für Laptop-/Tablet-Computer sowie Smartphones.

Hinzu kommen verhaltensbedingte Aspekte, denn der Mensch ist Schwachpunkt jeder Sicherheitsarchitektur:

- (a) Es sollten keine Programme aus unbekannter sowie nicht vertrauenswürdiger Quelle installiert werden, was Apps oder Plug-Ins einschließt. Wird am Bildschirm unvermittelt eine Zustimmung zu einer Programmausführung abgefragt, wird sie nicht erteilt, es sei denn, es ist ein Anlass und eine vertrauenswürdige Herkunft erkannt worden.
- (b) Emails, die Links enthalten und zur Eingabe von Daten auffordern, sind zuvor zu prüfen. Warnmerkmale sind: Absender nicht erkennbar oder unbekannt, mehrere nicht erkennbare Empfänger, keine personalisierte Anrede, schlechte Grammatik uvm. Im Zweifel sind solche Mails zu löschen. Bei zu großer Flut solcher Nachrichten sollte ein Spamfilter installiert werden. Die

⁶⁷ WLAN – *Wireless Local Area Network*, https://de.wikipedia.org/wiki/Wireless_Local_Area_Network.

⁶⁸ Bspw. mit *Bitlocker*, der Festplattenverschlüsselung des Betriebssystems *Windows*, die jedoch von Haus aus nicht unbedingt aktiviert ist; oder mit *Veracrypt* <https://www.veracrypt.fr/en/Downloads.html>; s. auch https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04435.html.

⁶⁹ WiFi LAN – *Wireless Local Area Network*, <https://de.wikipedia.org/wiki/Wi-Fi>.

Emailadressen der Beteiligten am Schiedsverfahren und andere bekannte Adressen können in sogenannte „White Lists“⁷⁰ eingetragen werden, die vermeiden, dass ausgefiltert wird.

(c) Dateianhänge unbekannter Herkunft sollten nicht geöffnet, sondern gelöscht werden. Zumindest sind sie vor dem Öffnen mit dem Virens Scanner zu untersuchen. Ausführbare Dateien sind ein Warnzeichen vor allem dann, wenn die Ausführbarkeit im sichtbaren Dateinamen verschleiert wird. Es ist möglich, das Betriebssystem so einzustellen, dass stets auch das Suffix, das die Art der Datei (zB .exe, .dll bei ausführbarem Code) angibt, angezeigt wird.

(d) Externe Datenträger sollten nur bei vertrauenswürdiger Quelle nach Untersuchung durch einen Virens Scanner eingelesen werden.

(e) Für den Zugriffsschutz ist stets – auch bei bloßer Aktivierung des Bildschirmschoners oder für einen kurzen Standby – ein Passwortschutz vorzusehen sowie auf zureichend komplexe Passwörter,⁷¹ die nicht für alles und jedes vergeben werden. Das kann durch Nutzung eines Passwortmanagers unterstützt werden.

(f) Zugang (auch körperlicher!) zu Datenspeichern bzw. einzelnen Verzeichnissen in denen sicherheitssensitive Daten gespeichert sind, sollte nur den Personen gewährt werden, die damit arbeiten müssen (*need-to-know*-Prinzip).

(g) Neben die elektronischen und verhaltensbedingten Schutzmaßnahmen, tritt der physische Schutz der Räume.

b) *Spezifische Sicherheitsaspekte im Schiedsverfahren*

Eine Besonderheit des Schiedsverfahrens ist, dass regelmäßig andere Beteiligte elektronische Informationen austauschen, also nicht auf eine stabile einheitliche Sicherheitsstruktur zurückgegriffen werden kann. Zudem können Sicherheitsregeln zwar festgelegt, aber deren Einhaltung schwer kontrolliert werden. Deshalb sollte jeder Beteiligte bei der Datenkommunikation mit den weiteren Beteiligten sein System im Grundsatz so schützen, wie das gegenüber unbekanntem Dritten erforderlich ist (siehe oben). Zusätzlich sollte eine Pflicht auferlegt werden, den weiteren Beteiligten Angriffe auf das eigene System, die tatsächlich oder nur möglicherweise die Daten des einzelnen Verfahrens betreffen, sofort mitzuteilen und bei der Gefahrengeringhaltung im notwendigen Umfang mitzuwirken.

c) *Schutz personenbezogener Daten (Grundlagen)*

Neben der Systemsicherheit zum Schutz der Vertraulichkeit und Datenintegrität sind im Schiedsverfahren durch alle Beteiligten jeweils eigenverantwortlich die Datenschutzbestimmungen (DGSVO) einzuhalten. Regelmäßig enthalten Beweisurkunden und andere Dokumente personenbezogene Daten Dritter, die nicht am Verfahren beteiligt sind. Sie dürfen nur bei Berechtigung zweckbestimmt gespeichert und verarbeitet werden, jede nicht (mehr) gedeckte Nutzung verlangt eine Einwilligung. Die Weitergabe an Dritte, insbesondere außerhalb der EU, ist problematisch. Nach Möglichkeit zu vermeiden ist die Weitergabe an nicht am Verfahren Beteiligte, insbesondere im Rahmen eines Outsourcing von Supportdienstleistungen durch Beteiligte an Dritte. Mit diesen ist eine Datenschutzvereinbarung zu treffen.⁷² Hier kann es zu Komplikationen kommen, die eine 100 % *Compliance* erschweren, wenn das Verfahren überhaupt durchgeführt werden soll. Der reibungsarme Verfahrensablauf hat in den Augen der Verfahrensbeteiligten sachgeben Vorrang.

⁷⁰ *White List*, https://de.wikipedia.org/wiki/Wei%C3%9Fe_Liste.

⁷¹ Zureichend komplexe Passwörter, https://www.bsi-fuerbuerger.de/BSIFB/DE/Empfehlungen/Passwoerter/passwoerter_node.html.

⁷² S. zB <https://www.datenschutz.rlp.de/de/themenfelder-themen/standarddatenschutzklauseln-der-eu-kommission-oder-einer-aufsichtsbehoerde/>.

Gleichwohl ist stets eine *Compliance* auf dem umständehalber höchstmöglichen Niveau herzustellen. Grundsätzlich gilt es deshalb, personenbezogene Daten nur sparsam zu generieren und zu nutzen, sie nicht in unnötigen Datenkopien zu speichern und sie in Ansehung von gesetzlichen Aufbewahrungsfristen frühestmöglich vollständig zu löschen. Weitere Einzelheiten zur Behandlung personenbezogener Daten können den einschlägigen Handreichungen der DIS entnommen werden.

10. Verfahrensrechtliche Aspekte der Nutzung von ICT im Schiedsverfahren

a) Einleitung des Schiedsverfahrens

Insbesondere, wenn im Verfahren aus Parteisicht erhöhte Anforderungen an den Geheimnisschutz, die Kommunikationssicherheit und die Nutzung von technischen Lösungen, wie virtuellen Datenräumen, in Betracht kommen, sollten die Parteien sich dazu auch schon vor Bildung des Schiedsgerichts im möglichen Umfang vorläufig abstimmen und sicherstellen, dass die in Betracht kommenden Schiedsrichter möglichst in der Lage und bereit sind, die beabsichtigten technischen Lösungen einzusetzen. Für den Fall einer Ersatzbestellung von Schiedsrichtern ist auch die DIS rechtzeitig über die Anforderungen zu informieren. Weil der Einsatz technischer Lösungen die Zusammenarbeit mit jedem Schiedsrichter erfordert, sollten die insoweit zu treffenden Maßnahmen aber erst im Zusammenwirken mit dem Schiedsgericht festgelegt werden.

b) Verfahrensmanagement, Zeitplan

Der Einsatz technischer Lösungen für den Schriftsataustausch und die Kommunikationssicherheit ist frühestmöglich nach Bildung des Schiedsgerichts abzustimmen. Die Verfahrensmanagementkonferenz (Art. 27.2 2018 DIS-Schiedsgerichtsordnung) ist der übliche aber auch letzte Zeitpunkt hierfür, auch wenn dieser Punkt getrennt zB telefonisch bzw. schriftlich abgehandelt werden kann.

Einzelheiten des Einsatzes von technischen Lösungen in der mündlichen Verhandlung können zu diesem Zeitpunkt noch nicht absehbar sein. Sie müssen dann rechtzeitig – regelmäßig wenigstens ein Monat – vor dem Termin in einer weiteren Verfahrensmanagementkonferenz geklärt werden, damit ausreichend Vorbereitungszeit zur Verfügung steht.

c) Anordnungen des Schiedsgerichts und Vereinbarungen

Die Erfahrung zeigt, dass der Einsatz technischer Lösungen die Kooperation aller Beteiligten einschließlich der Schiedsrichter erfordert, wenn es zu keinen absehbaren Störungen kommen soll. Regelmäßig sind nicht mit den Parteien einvernehmlich abgestimmte, insbesondere gegen den ausdrücklichen Widerstand einer Partei getroffene verfahrensleitende Anordnungen zu ICT-Aspekten nicht vorteilhaft. Gleichzeitig können sich abgestimmte technische Abläufe erfahrungsgemäß unvorhergesehen komplizieren. Deshalb sollten Regelungen zu technischen Kommunikationsabläufen und anderen ICT-Aspekten im Schiedsverfahren stets nicht als Parteivereinbarung, sondern vorzugsweise verfahrensleitende Anordnung mit Änderungsvorbehalt für das Schiedsgericht auf dessen eigene Initiative oder Parteiantrag erfolgen (Art. 21 2018 DIS-Schiedsgerichtsordnung). Jedoch wird regelmäßig vor der Änderung eine Abstimmung mit den betroffenen Verfahrensbeteiligten erfolgen.

Regelmäßig sind seitens der Parteien möglichst Zustimmungen zu folgenden Aspekten der Nutzung von technischen Lösungen einzuholen:

- (a) Zustimmung zur ausschließlich elektronischen Kommunikation von Schriftsätzen nebst Anlagen und anderen Schreiben im Verfahren;
- (b) Zustimmung zur unverschlüsselten elektronischen Kommunikation, wenn gewünscht (und zwar auch wenn nicht ausschließlich elektronisch kommuniziert wird);
- (c) Zustimmung zur Durchführung der Verhandlung per Video- oder Audiokonferenz, wenn gewünscht;

(d) Erklärung, dass die Parteien in das Verfahren nur solche personenbezogenen Daten einführen werden, die gesetzlich eingeführt werden dürfen (kein Zustimmungserfordernis) oder für die eine ausreichende Zustimmung vorliegt oder in Bezug auf welche das Schiedsgericht dies angeordnet hat.

In technischer Hinsicht kann den Parteien auferlegt werden:

(a) Sofortige Mitteilungen von Störungen (zB beschädigte Dateien, Ausfall des Email-Servers) oder sicherheitsrelevanten Angriffen auf ihr System (zB Virenfund, unbefugter Zugriff Dritter auf ihr System, etc.);

(b) Pflicht zur Mitwirkung bei der Folgenminimierung der Störungen und Vorfälle;

(c) Pflicht zur sofortigen Quittierung des Erhalts von elektronischen Mitteilungen/Schriftsätzen im Verfahren.

d) Spezifische Aspekte bei streitiger Integrität von Daten

Bei Dateien handelt es sich stets um Kopien. Das gilt auch für Schriftsätze und Schreiben, die nicht mit einer gültigen, qualifizierten elektronischen Signatur unterzeichnet sind. Wenn im Verfahren bestritten wird, dass ein in einer Datei wiedergegebenes Dokument echt oder unverfälscht ist, muss das gedruckte Original vorgelegt werden. Insoweit besteht kein Unterschied zu der Situation, in der die Authentizität einer Fotokopie bestritten wird. Allerdings werden im Wirtschaftsverkehr heute Emails und andere elektronische Daten unter den Beteiligten ausgetauscht, so dass lediglich elektronische „Originale“ existieren, selbst wenn ein Ausdruck vorgelegt wird. Hier muss bei erheblichem Bestreiten der Authentizität und Unverfälschtheit ein sachverständiger Computerforensiker in den Systemen einer oder mehrerer Parteien die Tatsachen feststellen; und zwar selbst dann, wenn im Schiedsverfahren keine ICT genutzt wird.

Jedenfalls dann, wenn derartige Fragen im Schiedsverfahren aufgeworfen werden, sind Anordnungen in Betracht zu ziehen, die weitere Veränderungen des relevanten Datenbestands und insbesondere ein Löschen untersagen.

In hoch streitigen Umgebungen kann die Unveränderlichkeit von Daten im Rahmen des Schiedsverfahrens durch den Einsatz von Prüfsummen (Hashes) geprüft und dokumentiert werden. Gängige, aus Unternehmensverkäufen bekannte Datenraumsoftware, kann dies ebenfalls gewährleisten.

III. Mustertexte & Checkliste

Die als **Anhang 1** beigefügten Mustertexte sind dem jeweiligen Einzelfall nach sorgfältiger Abwägung anzupassende Vorschläge, die auf einer Auswertung bekannter Regelungen in abgeschlossenen Schiedsverfahren beruhen. Es wird darauf hingewiesen, dass die Zweckmäßigkeit solcher oder ähnlicher Regelungen, vom einzelnen Schiedsverfahren abhängt. Jede Gewährleistung der DIS oder der Verfasser dieser Muster hinsichtlich der Richtigkeit und Brauchbarkeit der Mustertexte wird ausgeschlossen.

Die als **Anhang 2** beigefügte Checkliste enthält eine stichpunktartige Aufstellung etwa zu Verfahrensbeginn hinsichtlich des Einsatzes von ICT zu klärenden Punkten. Diese können, müssen aber nicht in jedem Fall, im einzelnen Verfahren relevant sein. Die Liste kann auch unvollständig sein.

Anhang 1

Illustrative ICT Klauseln

Kommunikation

Email

- (1) Schriftsätze und Anlagen werden per Email als Anhang in ein ZIP-Dateiarchiv gepackt an die von den Verfahrensbeteiligten für diesen Zweck angegebene Email-Adressen in einem Akt übermittelt. Bei erheblichem Datenumfang über <X MB> wird die Übermittlung durch Aufspaltung in mehrere ZIP-Archive und Emails, die im Betreff die Zahl und laufende Nummer der jeweiligen Sendung angeben, vorgenommen.
- (2) Die Übermittlung erfolgt gleichzeitig an alle Verfahrensbeteiligten. Zur Fristwahrung ist maßgebend das Übermittlungsdatum, in Zweifelsfällen der Eingang in den Mailserver des <Vorsitzenden/Einzelschiedsrichters> (CET).
- (3) Der Erhalt jeder Email wird durch Rückantwort „erhalten“ quittiert. Hat zum Fristablauf ein Verfahrensbeteiligter eine nach Verfahrenskalender fällige Eingabe nicht erhalten, oder stellt dieser fest, dass die übermittelten Dateien unvollständig oder technisch fehlerhaft sind, hat er dies den weiteren Verfahrensbeteiligten, insbesondere dem Schiedsgericht, unverzüglich, spätestens aber <X >Tage nach Fristablauf anzuzeigen. Mit danach erfolgenden Rügen ist der Beteiligte ausgeschlossen, es sei denn, das Schiedsgericht lässt sie ausnahmsweise zu.

Variante 1

- (4) Alle Beteiligten haben <in der Besprechung am TT.MM.YYYY> ausdrücklich darauf verzichtet, dass Emails und deren Anlagen verschlüsselt werden.

Variante 2

- (4) Alle Beteiligten haben <in der Besprechung am TT.MM.YYYY> ausdrücklich darauf verzichtet, dass Emails verschlüsselt werden. Jedoch sind die ZIP-Archive mit den Anlagen in AES256 oder besser zu verschlüsseln und mit einem Passwortschutz (wenigstens 8 Zeichen, davon mindestens ein Sonderzeichen und eine Zahl) zu versehen. Die Einzelheiten zum Austausch der Passwörter werden gesondert abgestimmt.

Variante 3

- (4) Alle Emails und ihre Anlagen werden mit <S/MIME / PGP> verschlüsselt übermittelt Die Einzelheiten zu den Schlüsseln werden gesondert abgestimmt.

SFTP

- (1) Schriftsätze und Anlagen werden mit dem dazu vom Schiedsgericht separat bestätigten sFTP Server in eine ZIP-Datei gepackt übermittelt, der an die von den Verfahrensbeteiligten für diesen Zweck angegebene Email-Adressen eine Nachricht versendet, dass die Eingabe zum Herunterladenbereit ist. Der Zugang zu dem sFTP-Server ist durch eine Nutzerkennung gesichert, die vorher oder spätestens gleichzeitig an die betroffenen Verfahrensbeteiligten übermittelt wurde. </Es wird eine Zwei-Faktoren Authentifizierung verwendet./> Die Einzelheiten zur Authentifizierung werden gesondert abgestimmt.
- (2) Die Übermittlung der Benachrichtigung über die Bereitstellung zum Herunterladen erfolgt gleichzeitig an alle Verfahrensbeteiligten. Zur Fristwahrung ist maßgebend das Übermittlungsdatum, in Zweifelsfällen der Eingang der Nachricht in den Mailserver des Vorsitzenden/Einzelschiedsrichters (CET).
- (3) Die anderen Verfahrensbeteiligten sind verpflichtet, die Eingabe sofort nach Erhalt der Nachricht über deren Bereitstellung auf dem sFTP Server herunterzuladen und diesen Vorgang per

Email mit „erhalten“ zu quittieren. Hat zum Fristablauf ein Verfahrensbeteiligter eine nach Verfahrenskalender erwartete Nachricht zum Herunterladen nicht erhalten, oder stellt er fest, dass kein Zugang auf den sFTP Server möglich ist oder dass die Übermittelten Dateien unvollständig oder technisch fehlerhaft sind, hat er dies den weiteren Verfahrensbeteiligten, insbesondere dem Schiedsgericht, unverzüglich, spätestens aber <X> Tage nach Fristablauf anzuzeigen. Mit danach erfolgenden Rügen ist der Beteiligte ausgeschlossen, es sei denn das Schiedsgericht lässt sie ausnahmsweise zu.

Datenraum

(1) Schriftsätze und Anlagen werden übermittelt, indem sie in den dazu vom Schiedsgericht separat bestätigten Datenraum und dem dort für diesen Beteiligten vorgesehen Verzeichnis hochgeladen werden, der an die von den Verfahrensbeteiligten für diesen Zweck angegebene Email-Adressen eine Nachricht versendet, dass die Eingabe im Datenraum verfügbar ist. Der Zugang zu dem Datenraum ist durch eine Nutzerkennung gesichert, die vorher oder spätestens gleichzeitig an die betroffenen Verfahrensbeteiligten übermittelt wurde. </Es wird eine Zwei-Faktoren Authentifizierung verwendet./>

(2) Die Übermittlung der Benachrichtigung über die Bereitstellung zum Herunterladen erfolgt gleichzeitig an alle Verfahrensbeteiligten. Zur Fristwahrung ist maßgebend das Hochladedatum; in Zweifelsfällen ist der Zeitstempel im Log des Datenraums maßgebend oder subsidiär der Eingang der Nachricht der Bereitstellung in den Mailserver des <Vorsitzen-den/Einzelschiedsrichters> (CET).

(3) Die anderen Verfahrensbeteiligten sind verpflichtet, die Eingabe sofort nach Erhalt der Nachricht über deren Bereitstellung im Datenraum herunterzuladen oder, je nach ihrer Wahl, von deren Inhalt vollständig Kenntnis zu nehmen. Hat zum Fristablauf ein Verfahrensbeteiligter die Nachricht über die Verfügbarkeit einer nach Verfahrenskalender erwarteten Eingabe im Datenraum nicht erhalten, oder stellt er fest, dass kein Zugang zu dem Verzeichnis im Datenraum möglich ist oder dass die hochgeladenen Dateien unvollständig oder technisch fehlerhaft sind, hat er dies den weiteren Verfahrensbeteiligten, insbesondere dem Schiedsgericht, unverzüglich, spätestens aber <X> Tage nach Fristablauf anzuzeigen. Mit danach erfolgenden Rügen ist der Beteiligte ausgeschlossen, es sei denn das Schiedsgericht lässt sie ausnahmsweise zu.

Videokonferenzen

(1) Grundsätzlich werden vorbehaltlich anderweitiger Anordnungen des Schiedsgerichts die verfahrensleitenden Termine in Form einer <Telefonkonferenz/Videokonferenz> unter Einsatz von <technische Plattform> durchgeführt. Die Einzelheiten dazu werden vom Schiedsgericht separat geregelt.

(2) Jede Partei stellt sicher, dass sie zu dem Termin die technischen Voraussetzungen für die Konferenz geschaffen hat und mit dem erforderlichen Netzwerk verbunden ist.

Mündliche Verhandlung ohne körperliche Präsenz

(1) Die mündliche Verhandlung wird vorbehaltlich anderweitiger Anordnungen des Schiedsgerichts in Form einer Videokonferenz unter Einsatz von <technische Plattform> durchgeführt. Die Einzelheiten dazu werden vom Schiedsgericht separat geregelt.

(2) Jede Partei stellt sicher, dass sie zu dem Termin die technischen Voraussetzungen für die Konferenz geschaffen hat und stabil mit dem erforderlichen Netzwerk verbunden ist.

(3) Die Zeugen/Sachverständigen werden in der Verhandlung ebenfalls über Videokonferenzschaltung gehört, bei der die in Ziffer (1) genannte technische Plattform genutzt wird. Die Partei, welche diese Person benannt hat, stellt sicher, dass dort, wo die betreffende Person zum Termin ist, die technischen Voraussetzungen für die Konferenz vorhanden sind und eine stabile Verbin-

dung mit dem erforderlichen Netzwerk besteht. In dem Raum, wo die Person sich befindet, soll jeweils auch ein Beauftragter der anderen Partei(en) anwesend sein. Die Partei, welche die Person benannt hat, gewährleistet, dass die physische Präsenz des Beauftragten möglich ist.

Präsenzverhandlung mit distanten Zeugen/Sachverständigen

(1) In der mündlichen Verhandlung können Zeugen und Sachverständige vorbehaltlich anderweitiger Anordnungen des Schiedsgerichts mittels einer Videokonferenz unter Einsatz von <technische Plattform> befragt werden. Die Einzelheiten dazu werden vom Schiedsgericht separat geregelt.

(2) Die Partei, welche diese Person benannt hat, stellt sicher, dass dort, wo die betreffende Person zum Termin ist, die technischen Voraussetzungen für die Konferenz vorhanden sind und eine stabile Verbindung mit dem erforderlichen Netzwerk besteht. In dem Raum, wo die Person sich befindet, soll jeweils auch ein Beauftragter der anderen Partei(en) anwesend sein. Die Partei, welche die Person benannt hat, gewährleistet, dass die physische Präsenz des Beauftragten möglich ist.

Änderungsvorbehalt Schiedsgericht

Alle Anordnungen zum Einsatz der Kommunikations- und Informationstechnologie in diesem Verfahren ergehen nach Konsultation mit den Parteien unter Änderungsvorbehalt seitens des Schiedsgerichts. Änderungen können auf begründeten Antrag einer Partei oder eigene Initiative des Schiedsgerichts nach Konsultation mit den Parteien erfolgen. In dringenden Notfällen kann von einer Konsultation abgesehen werden.

Datenschutz:

(1) Das Schiedsgericht weist die Verfahrensbeteiligten darauf hin, dass das Schiedsverfahren nicht von den anwendbaren Bestimmungen des Rechts zum Schutz personenbezogener Daten ausgenommen ist (in Deutschland DSGVO und BDGSG), für deren Einhaltung jeder Verfahrensbeteiligte auch in Zusammenhang mit diesem Schiedsverfahren unabhängig selbst verantwortlich bleibt.

(2) Das Schiedsgericht erwartet,

a) dass für alle in das Verfahren eingeführten personenbezogenen Daten eine Berechtigung für die Zwecke des Schiedsverfahrens vorliegt; sowie

b) nur solche personenbezogenen Daten eingeführt werden, die nach bestem Dafürhalten der sie einführenden Partei zur Anspruchsgeltendmachung bzw. Anspruchsabwehr notwendig sind. Dies schließt die Erwartung ein, dass in historischen Beweisstücken enthaltene personenbezogene Daten, die diese Voraussetzung nicht erfüllen und auch nicht zum Textverständnis erforderlich sind, geschwärzt oder pseudonymisiert werden.

(3) Das Schiedsgericht weist in diesem Zusammenhang darauf hin, dass die genannten gesetzlichen Regeln keine Verfahrensregeln sind, grundsätzlich prozessuale Zulässigkeitsfragen nicht regeln, und auch keine anderen als die gesetzlichen Pflichten unter den Verfahrensbeteiligten begründen.

(4) Das Schiedsgericht behält sich gleichwohl im Rahmen seiner allgemeinen Regelungsbefugnisse vor, auf eigene Initiative oder Antrag Maßnahmen zu treffen, um die Integrität des Verfahrens und seines Ablaufs auch in Bezug auf personenbezogene Daten zu regeln.

Anhang 2

CHECKLISTE INFORMATIONS- UND KOMMUNIKATIONSTECHNOLOGIE & SCHIEDSVERFAHREN

(für Schiedsgericht & Parteien)*

A. Klärungsbedürftige Vorfragen

- 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 fristwährenden 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 dh („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, zB als komprimiertes, passwortgeschütztes Dateiarchiv (ggf. Verschlüsselungsstandard, Passwortaustausch)?
 - Zu berücksichtigende andere technische Einflussfaktoren (Volumenbegrenzungen, Spamfilter, etc.)?
 - Regeln zu Fristwahrung, Eingangsbestätigung?
- Per sFTP-Server:
 - Welcher Server, wie gesichert, Passwortaustausch, Format der hochzuladenden Dateien (zB passwortgeschütztes Dateiarchiv oder einzelne, ungepackte Dateien)?
 - Regeln zu Fristwahrung, Pflicht zum Herunterladen, Eingangsbestätigung, etc.?
- Per Datenraum in der Cloud:

* Diese Checkliste ist das Arbeitsprodukt der in der Vorbemerkung genannten Arbeitsgruppe des DIS-Beirats und wird von der DIS gesondert veröffentlicht werden. Sie wird hier mit Genehmigung der DIS vorab abgedruckt.

- 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 (zB Flash Memory (USB), CD, DVD, Blu-ray, portable Festplatte)?
 - Klärung technischer Beschränkungen, zB 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 (zB 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 (zB 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 Tonmittschnitts 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 (zB 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; zB 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.).