Datenschutz im Schiedsverfahren – die Rolle des Schiedsgerichts[1]

Von MMag. Anja Cervenka und Mag. Philipp Schwarz, Wien*

Die Datenschutz-Grundverordnung (DSGVO) ist auf die Datenverarbeitung in Schiedsverfahren anwendbar. Parteien, deren Vertreter, Schiedsinstitutionen und Schiedsgericht verarbeiten während des Verfahrens personenbezogene Daten in großem Umfang und sind damit Adressat der Pflichten der DSGVO. Aufgrund seiner besonderen Einflussmöglichkeiten auf die Gestaltung des Verfahrens, kommt dem Schiedsgericht eine Schlüsselrolle im Zusammenhang mit der Einhaltung der datenschutzrechtlichen Bestimmungen zu. Um dieser Rolle gerecht zu werden, hat das Schiedsgericht so früh als möglich gemeinsam mit den Parteien ein Datenschutz-Protokoll zu erstellen. Darin sind sämtliche datenschutzrechtlichen Überlegungen anzuführen. Insbes. sind Vorkehrungen zu den Informationspflichten, den datenschutzrechtlichen Aspekten des Beweisverfahrens und der Datensicherheit zu treffen.

The General Data Protection Regulation (GDPR) applies to the processing of data in arbitration proceedings, in the course of which parties, their representatives, arbitral institutions, and arbitral tribunals process a considerable amount of personal data. Accordingly, all actors are subject to the obligations under the GDPR. Due to its particular influence on the conduct of the arbitral process, the arbitral tribunal takes center-stage in creating a process to safeguard compliance with the GDPR. To that end, the arbitral tribunal will as soon as possible set up a data protection protocol together with the parties of the proceedings. Therein it should address all data protection considerations. In particular, the arbitral tribunal should take precautions with regard to the disclosure obligations, the data protection aspects of the taking of evidence, and data security.

I. Einleitung

Die Anwendbarkeit der Datenschutz-Grundverordnung[2] (DSGVO) im Mai 2018 führte, nicht zuletzt aufgrund verschärfter Strafbestimmungen, zu einer tiefgehenden Auseinandersetzung mit Datenschutz in nahezu allen Rechtsbereichen.

Durch den weiten Anwendungsbereich sind beinahe sämtliche Rechtsbereiche von der DSGVO betroffen – so auch Schiedsverfahren. Tatsächlich verarbeiten alle Hauptakteure eines Schiedsverfahrens, wie Parteien,

Parteienvertreter, Schiedsinstitutionen und Schiedsrichter, im Laufe des Verfahrens personenbezogene Daten in großem Umfang. Die Schiedsszene hat die Relevanz des Datenschutzrechts bereits erkannt. Schiedsinstitutionen haben Tipps im Umgang mit personenbezogenen Daten für Beteiligte im Schiedsverfahren herausgegeben.[3] Der *International Council for Commercial Arbitration* (ICCA) und die *International Bar Association* (IBA) haben ferner die Veröffentlichung eines umfassenden Leitfadens zum Thema Datenschutz

angekündigt.[4] Daneben findet in der Literatur zunehmend eine Auseinandersetzung mit datenschutzrechtlichen Aspekten im Zusammenhang mit Schiedsverfahren statt.[5]

Da sich die datenschutzrechtlichen Pflichten der Parteien sowie deren Vertreter durch die Durchführung eines Schiedsverfahrens nur unwesentlich verändern und sich Schiedsinstitutionen (intern) intensiv mit deren Verpflichtungen auseinandersetzen, rückt dieser Artikel die datenschutzrechtliche Rolle des Schiedsgerichts in den Fokus.

Nach einer Besprechung der Anwendung der DSGVO auf die schiedsrichterliche Tätigkeit (II.) wird das Schiedsgericht als Verantwortlicher qualifiziert (III.). Anschließend wird die Rechtsgrundlage der Verarbeitung personenbezogener Daten durch das Schiedsgericht (IV.) und die datenschutzrechtliche Rolle des Schiedsgerichts anhand ausgewählter Themen veranschaulicht (V.). Schließlich werden die potentiellen Folgen von Datenschutzverletzungen in Ausblick gestellt (VI.)

II. Anwendung der DSGVO auf die schiedsrichterliche Tätigkeit

1. Personenbezogene Daten im Schiedsverfahren

Unter *„personenbezogenen Daten*" werden sämtliche Informationen verstanden, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen (Art. 4 Abs. 1). Daten juristischer Personen sind vom sachlichen Anwendungsbereich der DSGVO ausgenommen.[6] Mit dem Begriff *„Verarbeiten*" meint die DSGVO nahezu jeden erdenklichen Vorgang im Zusammenhang mit personenbezogenen Daten (Art. 4 Abs. 2).

Aufgabe des Schiedsgerichts ist es, anhand der eingebrachten Schriftsätze und der vorgelegten bzw. eingeholten Beweise den Sachverhalt einer Schiedsstreitigkeit festzustellen und diesen rechtlich zu würdigen. Besonders im Beweisverfahren werden in großem Umfang personenbezogene Daten an das Schiedsgericht übermittelt. Aber auch die Schriftsätze enthalten regelmäßig personenbezogene Daten. Der Erhalt, die Speicherung bzw. Aufbewahrung, die Durchsicht und die Beurteilung der vorgelegten Unterlagen sind für sich genommen bereits Verarbeitungen personenbezogener Daten iSd DSGVO. Da die vom Schiedsgericht verfassten prozessleitenden Verfügungen und letztlich auch der Schiedsspruch notwendig Bezug auf die vorgelegten Unterlagen nehmen, werden auch durch deren Erstellung und Erlass personenbezogene Daten verarbeitet. Sämtliche dieser Vorgänge müssen daher den Anforderungen der DSGVO standhalten.

2. Räumlicher Anwendungsbereich

Schiedsrichter unterliegen jedenfalls dann den Bestimmungen der DSGVO, wenn ihre Niederlassung innerhalb der Europäischen Union oder des Europäischen Wirtschaftsraums (EWR)[7] liegt. Abgestellt wird dabei nicht auf Formalien, sondern auf jenen Ort, an dem die effektive und tatsächliche Ausübung einer Tätigkeit durch eine feste Einrichtung stattfindet.[8] Trifft dies nur für ein Mitglied des Schiedsgerichts zu, so unterliegen deshalb nicht die anderen Mitglieder und das gesamte Schiedsverfahren der DSGVO.[9] Praktisch hat aber freilich die Anwendbarkeit auf nur einen der Schiedsrichter auch Implikationen für das gesamte Verfahren, etwa in Zusammenhang mit Datensicherheit.[10] Auch ein Schiedsort oder Besprechungen und mündliche Verhandlungen innerhalb der Union führen für sich genommen ohne weitere Anknüpfungspunkte daher nicht automatisch zur Anwendbarkeit der DSGVO. Maßgeblich ist vielmehr vornehmlich die Niederlassung des Schiedsrichters durch eine feste Einrichtung.

Ist ein Schiedsrichter nicht in der Union angesiedelt, kommen die Bestimmungen der DSGVO nichtsdestotrotz unabhängig vom Ort der Datenverarbeitung zur Anwendung, soweit die Tätigkeit im Rahmen einer Niederlassung innerhalb der Union erfolgt (Art. 3 Abs. 1). Ein möglicher Anwendungsfall ergibt sich, wenn ein Schiedsrichter seine Niederlassung zwar außerhalb der Union hat, er aber organisatorisch einer innerhalb der Union niedergelassenen Kanzlei zugehört. Unseres Erachtens sprechen jedoch die besseren Gründe dafür, dass in einer solchen Konstellation ohne weitere Anknüpfungspunkte das Schiedsgericht nicht

den Bestimmungen der DSGVO unterliegt. Dies da vornehmlich der Schiedsrichter selbst und nicht die dahinterstehende Kanzlei Adressat der datenschutzrechtlichen Bestimmungen im Schiedsverfahren ist (III.). Wird die Kanzlei als Auftragsverarbeiter auf Weisung des Schiedsrichters tätig, ist dies nicht ausreichend, um die Bestimmungen der DSGVO auch auf den Schiedsrichter als datenschutzrechtlichen Verantwortlichen anzuwenden.[11] Auch hat der Europäische Gerichtshof (EuGH) festgehalten, dass es zwar nicht darauf ankommt, ob die Niederlassung selbst die Datenverarbeitung vornimmt, sondern ob die Datenverarbeitung untrennbar mit der relevanten Tätigkeit in Zusammenhang steht.[12] Da die schiedsrichterliche Datenverarbeitung unabhängig erfolgt und dabei lediglich unter Umständen die Kanzleiinfrastruktur unterstützend genutzt wird, besteht unseres Erachtens kein untrennbarer Zusammenhang. Ebenfalls wohl nicht ausreichend für die Anwendbarkeit der DSGVO ist es, wenn das Verfahren unter den Regeln einer Schiedsinstitution innerhalb der Union durchgeführt und durch diese administriert wird.

Auch vor Durchführung eines Schiedsverfahrens kann ein Schiedsrichter bereits den Regeln der DSGVO unterliegen, soweit dieser seine Tätigkeit auf den Markt innerhalb der Union ausrichtet und sich dieses Angebot zumindest teilweise auch auf natürliche Personen bezieht.[13]

Liegt lediglich der Schiedsort innerhalb der Union und bestehen sonst keine relevanten Anknüpfungspunkte des Schiedsgerichts zur Union, findet die DSGVO keine direkte Anwendung. Denkbar ist jedoch, dass die DSGVO zum europäischen *ordre public* gezählt wird und eine Verletzung im Rahmen eines Aufhebungsverfahrens aufgegriffen werden kann (VI.2).

III. Das Schiedsgericht als datenschutzrechtlicher Verantwortlicher

Zentrale Rolle im Datenschutzrecht ist die des Verantwortlichen; ihn treffen neben umfassenden Dokumentationspflichten insbes. Informations- und Auskunftspflichten gegenüber natürlichen Personen, deren personenbezogene Daten verarbeitet werden.

Neben den beteiligten Schiedsinstitutionen und Parteienvertretern liegt es allen voran am Schiedsgericht, einen Rahmen zum Schutz personenbezogener Daten im Verfahren zu schaffen. Die einzelnen Schiedsrichter sind ohne Zweifel als Verantwortliche im Sinne der DSGVO tätig, weil sie über Mittel und Zweck der Datenverarbeitung entscheiden. Offen bleibt, ob dabei die dahinterstehende Kanzlei oder der jeweilige Schiedsrichter Verantwortlicher ist. Der Schiedsrichtervertrag besteht zwischen den Parteien und dem konkreten Schiedsrichter und das Amt des Schiedsrichters ist darüber hinaus auch höchstpersönlich gestaltet.[14] Es ist daher unseres Erachtens nur konsequent, dass der jeweilige

Schiedsrichter selbst datenschutzrechtlich Verantwortlicher ist. Freilich kann bei Nutzung der Kanzleiinfrastruktur diese datenschutzrechtlich als Auftragsverarbeiter (Art. 4 Z. 8)[15] oder allenfalls sogar Verantwortlicher tätig werden. Zur Gewährleistung von Betroffenenrechten interpretiert der EuGH den Begriff des Verantwortlichen jedoch weit.[16] Vor diesem Verständnis und der notwendigen Datenverarbeitung bei Nutzung der Kanzleiinfrastruktur besteht hier also Argumentationsspielraum. Diese Unterscheidung ist insbes. für die Frage der Anwendbarkeit der DSGVO sowie bei Bemessung einer Strafe im Fall einer Datenschutzverletzung relevant.

Um als Verantwortlicher den datenschutzrechtlichen Pflichten nachzukommen und getroffene Vorkehrungen zu dokumentieren, sollte das Schiedsgericht die Parteien so früh als möglich, idR während der *Case Management Conference*, zum Thema Datenschutz hören, um den Abschluss eines Datenschutz-Protokolls zu erreichen.[17] Das Datenschutz-Protokoll kann auch die Form einer Parteienvereinbarung, einer Erklärung oder einer prozessleitenden Verfügung annehmen. Die ICC empfiehlt dieses in die *Terms of Reference* aufzunehmen.[18]

Legen mehrere Personen gemeinsam die Zwecke und die Mittel einer Verarbeitung fest, sind sie gemeinsame Verantwortliche und schließen eine Vereinbarung ab, die vorsieht, wer welchen datenschutzrechtlichen Pflichten nachkommt (Art. 26). Die Rolle des gemeinsamen Verantwortlichen wurde in dieser Form mit der DSGVO neu eingeführt und sorgt bislang für Verwirrung.

Besteht das Schiedsgericht aus mehreren Schiedsrichtern und unterliegen diese der DSGVO,[19] könnten sie als gemeinsame Verantwortliche qualifiziert werden. Auch für sämtliche Beteiligten im Schiedsverfahren wurde bereits angedacht, dass diese als gemeinsame Verantwortliche handeln.[20] Die DIS vertritt generell die Position, die gesetzlich festgeschriebene Unabhängigkeit des Schiedsrichters und dessen Verfahrenshoheit spreche gegen die Rolle des gemeinsamen Verantwortlichen.[21] Dies trifft jedenfalls bei den Beteiligten des Schiedsverfahrens bereits aufgrund der unterschiedlichen Interessen und Mittel in der Datenverarbeitung zu. Unseres Erachtens sind Parteien und Schiedsrichter

jedenfalls unabhängig voneinander verantwortlich. Offen ist jedoch wie es sich bei mehreren Mitgliedern eines Schiedsgerichts verhält.[22] Freilich haben die Mitglieder des Schiedsgerichts im Detail Handlungsfreiheit, wie sie die Daten verarbeiten, der übergeordnete Zweck und die Mittel sind aber durch die gemeinsame Entscheidungsfindung festgelegt. Der EuGH wendet den Begriff des Verantwortlichen großzügig an[23] und nimmt gemeinsame Verantwortlichkeit auch an, wenn die Akteure in unterschiedlichem Ausmaß und Phasen in die Verarbeitung einbezogen sind.[24] Dies spricht dafür, dass die Mitglieder des Schiedsgerichts datenschutzrechtlich gemeinsame Verantwortliche sind. Im Übrigen bringt diese Rolle für das Schiedsgericht zumindest eine organisatorische Vereinfachung, weil nicht jedes Mitglied eigenständig datenschutzrechtlichen Pflichten nachkommen muss, sondern diese gebündelt werden können. Konkret bedeutet das für das Schiedsgericht, dass dieses sämtlichen Betroffenen eine Vereinbarung gemäß Art. 26 DSGVO vorzulegen hat, in dem es ua darlegt, welches Mitglied den Betroffenenrechten und Informationspflichten nachkommt. In der Regel wird der Vorsitzende Anlaufstelle für die Parteien oder Betroffenen sein. Betroffene können aber auch gegenüber den anderen Mitgliedern des

Schiedsgerichts ihre Ansprüche geltend machen, die gesamtschuldnerisch haften (Art. 26 Abs. 3). Wie auch mit den anderen datenschutzrechtlichen Pflichten, sollte die Vereinbarung in das Datenschutz-Protokoll aufgenommen werden.

IV. Rechtsgrundlage für die Verarbeitung personenbezogener Daten durch das Schiedsgericht

Im Rechtsrahmen der DSGVO ist eine Verarbeitung personenbezogener Daten nur dann rechtmäßig, wenn mindestens eine der taxativ angeführten Bedingungen erfüllt ist (Art. 6 und 9). Aus Sicht des Schiedsgerichts kommen dabei potentiell die Einwilligung der betroffenen Person (Art. 6 Abs. 1 lit. a), die Erfüllung einer vertraglichen Pflicht (Art. 6 Abs. 1 lit. b), die Erfüllung einer gesetzlichen Pflicht (Art. 6 Abs. 1 lit. c) und die Wahrung besonderer Interessen Dritter (Art. 6 Abs. 1 lit. f) in Betracht. Da das Schiedsgericht die Einhaltung seiner datenschutzrechtlichen Pflichten auch nachweisen können muss (Art. 5 Abs. 2), empfiehlt es sich, die Rechtsgrundlage der Datenverarbeitung im Datenschutz-Protokoll anzuführen.

Die Einwilligung der betroffenen Personen scheidet sowohl aus rechtlichen, als auch aus praktischen Gründen als Rechtsgrundlage aus. Zum einen sind die rechtlichen Anforderungen an das Vorliegen einer Einwilligung hoch,[25] zum anderen kann die Einwilligung jederzeit widerrufen werden (Art. 7 Abs. 3). Dadurch entstehen praktische Schwierigkeiten bezüglich Daten, die bereits Eingang in das Schiedsverfahren gefunden haben und deren Verarbeitung nunmehr unzulässig ist. Darüber hinaus ist die Einholung der Einwilligung sämtlicher betroffenen Personen für das Schiedsgericht praktisch schlicht untunlich.

Da die Parteien eines Schiedsverfahrens mit den Mitgliedern des Schiedsgerichts einen Schiedsrichtervertrag abschließen, ist die Verarbeitung der personenbezogenen Daten der Parteien zur Erfüllung ebendieses Vertrages erforderlich und daher rechtmäßig (Art. 6 Abs. 1 lit. b). Die Rechtmäßigkeit der Verarbeitung personenbezogener Daten von Dritten kann dadurch jedoch nicht gerechtfertigt werden.[26] Der Anwendungsbereich dieser Rechtsgrundlage ist insofern eng und nicht geeignet, sämtliche Verarbeitungen zu rechtfertigen.

Auch eine Rechtfertigung zur Datenverarbeitung aufgrund eines Gesetzes scheidet aus. Es besteht keine Rechtspflicht kraft objektiven Rechts zur Ausübung des Schiedsrichteramts. Das Schiedsgericht wird vielmehr ausschließlich aufgrund vertraglicher Vereinbarung tätig. Folglich kann die Rechtmäßigkeit der Verarbeitung personenbezogener Daten durch das Schiedsgericht nicht auf die Erfüllung einer Rechtspflicht gestützt werden.[27]

Allerdings ist eine Verarbeitung gemäß Art. 6 Abs. 1 lit. f DSGVO auch dann rechtmäßig, wenn diese zur Wahrung berechtigter Interessen des Verantwortlichen oder eines Dritten erforderlich ist. Die DSGVO erkennt die Geltendmachung, Ausübung und Verteidigung von Rechtsansprüchen auch in außergerichtlichen Verfahren implizit als berechtigtes Interesse an.[28] Aus Art. 21 DSGVO folgt sogar, dass es sich dabei um ein *„eo ipso zwingend schutzwürdig[es] Interesse*" handelt.[29] Die Parteien des Schiedsverfahrens haben somit ein berechtigtes Interesse an der Durchführung eines Schiedsverfahrens. Zur Wahrung dieses berechtigten Interesses ist die Verarbeitung der im Schiedsverfahren aufkommenden personenbezogenen Daten durch das Schiedsgericht erforderlich.[30] Die Verarbeitung durch das Schiedsgericht ist daher gemäß Art. 6 Arb. 1 lit. f DSGVO rechtmäßig. Da es sich bei der Geltendmachung, Ausübung und Verteidigung von Rechtsansprüchen um ein zwingend schutzwürdiges Interesse handelt, bedarf es keiner umfassenden Interessenabwägung im Einzelfall und kann auch nicht erfolgreich Widerspruch gegen die Verarbeitung erhoben werden.[31]

V. Pflichten des Schiedsgerichts

Dem Schiedsgericht kommt eine Schlüsselrolle im Zusammenhang mit der Einhaltung der datenschutzrechtlichen Bestimmungen zu. Zum einen ist es, wie oben dargelegt, Verantwortlicher und daher unmittelbar Adressat datenschutzrechtlicher Pflichten, zum anderen übt das Schiedsgericht grundlegendes Ermessen bei der Gestaltung des Schiedsverfahrens aus. Das Schiedsgericht kann dadurch maßgeblich auf die Schaffung eines Rahmens zum Schutz personenbezogener Daten im Verfahren einwirken und die Einhaltung der Grundsätze für die Verarbeitung personenbezogener Daten, wie insbes. den Grundsatz der Datenminimierung und der Integrität und Vertraulichkeit, gewährleisten.

Zu diesem Zweck sollten Vorkehrungen zu Informationspflichten (1.), zu datenschutzrechtlichen Aspekten des Beweisverfahrens (2.) und zur Datensicherheit (3.) sowie weiteren Aspekten (4.) getroffen werden. Die Ergebnisse können sodann in das Datenschutz-Protokoll aufgenommen werden.

1. Information über die Datenverarbeitung an Betroffene

Verantwortliche haben gemäß Art. 13 und 14 DSGVO eine umfassende Informationspflicht gegenüber den Betroffenen über die Verarbeitung ihrer Daten. Im Rahmen einer Öffnungsklausel haben Mitgliedstaaten die Möglichkeit, die Rechte betroffener Personen zum Schutz von Gerichtsverfahren und der Unabhängigkeit der Justiz (Art. 23 Abs. 1 lit. f)[32] sowie zur Durchsetzung zivilrechtlicher Ansprüche (Art. 23 Abs. 1 lit. j) zu beschränken. Auf dieser Basis besteht Argumentationsspielraum für Mitgliedstaaten, datenschutzrechtliche Pflichten des Schiedsgerichts zu minimieren.[33] Soweit ersichtlich hat bislang kein Mitgliedstaat diese Möglichkeit konkret für Schiedsverfahren wahrgenommen.[34] Nichtsdestotrotz sollten die nationalen Durchführungsgesetze beachtet werden. Für Deutschland können sich Schiedsrichter etwa im Einzelfall auf die in §§ 29, 32 und 33 Bundesdatenschutzgesetz festgelegten Ausnahmen stützen.

Das Schiedsgericht erhebt in der Regel personenbezogene Daten nicht bei den Betroffenen selbst, sondern werden ihm diese durch Parteienvertreter oder zugezogene Sachverständige übermittelt. Es unterliegt somit einer eingeschränkten Informationspflicht nach Art. 14 DSGVO und kann von den darin vorgesehenen Ausnahmen Gebrauch machen.

Information kann ua unterbleiben, soweit der Betroffene bereits über die Informationen verfügt (Art. 14 Abs. 5 lit. a). Im Rahmen des Datenschutz-Protokolls sollte das Schiedsgericht daher festlegen, dass es keine Informationspflicht trifft, weil die Parteien bei den von ihnen übermittelten personenbezogenen Daten ihren Informationsverpflichtungen bereits nachgekommen sind oder die Betroffenen entsprechend informieren werden. Auch praktische Erwägungen sprechen dafür, weil es den Parteien obliegt, welche Daten sie im weiteren Schiedsverfahren übermitteln und den Betroffenen in der Regel auch näherstehen.

Als weitere Ausnahme kommt in Betracht, dass eine Informationsweitergabe an die Betroffenen die Ziele der Verarbeitung unmöglich macht oder zumindest ernsthaft beeinträchtigt (Art. 14 Abs. 5 lit. b). Sprechen daher im Einzelfall Vertraulichkeitserwägungen dagegen, Betroffene vom anhängigen Schiedsverfahren zu informieren, kann sich das

Schiedsgericht auch auf diesen Ausnahmegrund stützen. Das Schiedsgericht sollte hierfür seine Erwägungen konkret dokumentieren, ein pauschaler Verweis auf die Vertraulichkeit von Schiedsverfahren ist unseres Erachtens nicht ausreichend.

Schlussendlich ist anzumerken, dass ein anwaltliches Berufsgeheimnis für die schiedsrichterliche Tätigkeit nicht zum Ausschluss der datenschutzrechtlichen Informationspflicht iSd Art. 14 Abs. 5 lit. d DSGVO führt.[35]

2. Datensicherheit

Im Bereich der Datensicherheit gab es aufgrund wiederholter Cyberangriffe im Zusammenhang mit Schiedsverfahren[36] vermehrt Bestrebungen, ein einheitliches Datensicherheitssystem zu entwickeln.[37] Besonders das von ICCA, NY Bar und CPR veröffentlichte *Protocol on Cybersecurity in International Arbitration* (*2020 Edition*)[38] bietet einen guten Anhaltspunkt, wie Datensicherheit praktisch umgesetzt werden kann. Zu berücksichtigen ist allerdings, dass das *Protocol* nicht in Umsetzung der DSGVO entworfen wurde und ausschließlich *cybersecurity* betrifft. Das *Protocol* ist daher gemeinsam mit den zwingenden Bestimmungen der DSGVO zu lesen.

Gemäß Art. 32 DSGVO hat der Verantwortliche technische und organisatorische Maßnahmen zu ergreifen, um die Vertraulichkeit,[39] die Integrität,[40] die

Verfügbarkeit[41] und die Belastbarkeit[42] der verarbeiteten personenbezogenen Daten zu gewährleisten. Das angestrebte Schutzniveau hängt dabei von mehreren Faktoren ab: (i) dem Stand der Technik, (ii) den Implementierungskosten, (iii) der Art, den Umständen und dem Zweck der Verarbeitung sowie (iv) der Schwere und der Eintrittswahrscheinlichkeit des Risikos für die Rechte der betroffenen Person (Art. 32 Abs. 1). Die konkrete Umsetzung der Datensicherheit ist demnach in höchstem Grade einzelfallabhängig und verfolgt einen risikobasierten Ansatz.

Um ein einheitliches Schutzniveau zu erreichen, sollte das Schiedsgericht so früh als möglich gemeinsam mit den Parteien eine Risikoanalyse durchführen.[43] Dabei sind die zu verarbeitenden Daten, die Eintrittswahrscheinlichkeit und die Schwere des Risikos zu identifizieren. Anhand der Risikoanalyse können konkrete Maßnahmen zur Gewährleistung der Datensicherheit festgelegt werden.[44] Diese Maßnahmen sollten nicht nur technische Einrichtungen wie verschlüsselte Datenübermittlung vorsehen. Vielmehr sollten auch Prozesse zur Erkennung von Sicherheitsvorfällen, deren Prüfung und Behandlung implementiert werden.[45] Die Auswahl der technischen[46] und organisatorischen Maßnahmen obliegt in erster Linie der Vereinbarung der Parteien.[47] Mangels Einigung oder aufgrund eines unzureichenden Schutzniveaus kann das Schiedsgericht jedoch laufend die Implementierung anderer Maßnahmen verfügen.[48] Die Ergebnisse der Risikoanalyse und die ergriffenen Maßnahmen sind im Datenschutz-Protokoll festzuhalten.

Sowohl die DSGVO als auch das *Protocol on Cybersecurity in International Arbitration* machen das Schutzniveau von den Implementierungskosten abhängig.[49] Aufgrund von Unterschieden zwischen den Ressourcen der Parteien, deren Vertretern, der Schiedsinstitution und dem Schiedsgericht ist die Erreichung eines einheitlichen Datensicherheitsstandards in der Schiedsgerichtsbarkeit unwahrscheinlich. Es ist daher zu begrüßen, dass

Schiedsinstitutionen, wie bspw. die SCC,[50] ihren Nutzern sichere Datenräume anbieten. Schiedsinstitutionen nehmen damit eine zentrale Rolle im Zusammenhang mit Datensicherheit in der Schiedsgerichtsbarkeit ein.

3. Beweisverfahren

Während des Beweisverfahrens wird der Großteil der personenbezogenen Daten verarbeitet. Das Beweisverfahren steht dabei in einem gewissen Spannungsverhältnis zum Grundsatz der Datenminimierung.[51] Auf der einen Seite haben die Parteien Interesse daran, umfangreiche Beweise anzubieten und im Rahmen der *document production* von der Gegenseite vorgelegt zu erhalten, um deren Tatsachen- oder Rechtsvortrag zu stützen. Auf der anderen Seite müssen personenbezogene Daten aufgrund des Grundsatzes der Datenminimierung dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein (Art. 5 Abs. 1 lit. c). Das Schiedsgericht kann erheblich dazu beitragen, dieses Spannungsverhältnis auszugleichen.

Im Zusammenhang mit der freiwilligen Urkundenvorlage durch die Parteien sollte das Schiedsgericht den Parteien in der prozessleitenden Verfügung Nr. 1 die Beachtung des Grundsatzes der Datenminimierung auftragen. Lediglich jene Beweise sollen angeboten werden, die für den Beweis des entsprechenden Vorbringens tatsächlich erforderlich sind. Die Verfassung eines Schiedsauftrags, wie dieser in ICC-Verfahren vorgesehen ist,[52] in dem die zu entscheidenden Streitfragen konkretisiert werden, ermöglicht es ferner die entscheidungsrelevanten Beweisthemen einzuschränken.

Im Zusammenhang mit der *document production* ist das Schiedsgericht angehalten, die Bestimmtheit des Vorlageantrags genau zu prüfen und nur jenen Anträgen stattzugeben, die Urkunden betreffen, die tatsächlich für das Schiedsverfahren relevant sind. Denkbar wäre ferner, das Ausmaß der *document production* entsprechend den Prager Regeln auf ein Minimum zu reduzieren.[53]

Sollten trotz der ergriffenen Vorkehrungen Urkunden mit für das Schiedsverfahren unerheblichen personenbezogenen Daten vorgelegt werden, stellt sich die Frage, ob das Schiedsgericht die entsprechenden Beweisanträge aufgrund des Grundsatzes der Datenminimierung zurückzuweisen hat. Dies wird im Einzelfall mit der Pflicht des Schiedsgerichts, das rechtliche Gehör der Parteien zu wahren und ein faires Verfahren durchzuführen, abzuwägen sein. Allgemein kann jedoch festgehalten werden, dass sich die Datenminimierung am Zweck der Verarbeitung orientiert. Der Zweck der Verarbeitung durch das Schiedsgericht ist die materielle Wahrheitsfindung. Insofern wird das Schiedsgericht sämtliche ihm vorgelegte Urkunden würdigen dürfen – auch wenn diese keine Relevanz für den Ausgang des Verfahrens haben.

Aus dem Grundsatz der Datenminimierung folgt freilich auch, dass das Schiedsgericht nur jene personenbezogenen Daten in prozessleitende Verfügungen und den Schiedsspruch aufnehmen darf, die für deren Erlass tatsächlich notwendig sind.

4. Weitere Aspekte

Zu beachten ist, dass das Schiedsgericht noch weitere datenschutzrechtliche Pflichten treffen, deren Darstellung jedoch den Umfang dieses Artikels sprengen würde. Hierzu gehören insbes. die Führung eines Verarbeitungsverzeichnisses (Art. 30), Meldungen von Datenschutzverletzungen an die zuständige Datenschutzbehörde und in Einzelfällen an den Betroffenen (Art. 33), bei besonderen Risiken der Verarbeitung Durchführung einer Datenschutz-Folgenabschätzung (Art. 35), Überprüfung der Datenübermittlung in Drittstaaten (Kap. V),[54] sowie das Abschließen von Vereinbarungen mit Auftragsverarbeitern (Art. 28).[55] Macht ein Betroffener Rechte nach Art. 15 ff. DSGVO geltend, so hat das Schiedsgericht im Einzelnen festzulegen, ob sie der Anfrage nachkommen muss oder sich auf eine Ausnahmenbestimmung stützen kann.

VI. Folgen einer Datenschutzverletzung durch das Schiedsgericht

Sollten während eines Schiedsverfahrens die Rechte der betroffenen Personen verletzt werden, kann das Schiedsgericht zum einen Adressat der datenschutzrechtlichen Strafbestimmungen werden (1.). Zum anderen stellt sich die Frage, ob Datenschutzverletzungen Auswirkungen auf die Gültigkeit des Schiedsspruchs haben können (2.).

1. Strafen bei Datenschutzverletzung durch das Schiedsgericht

In das allgemeine Bewusstsein gelangt sind vor allem die hohen Strafsummen (Art. 83 Abs. 4, 5, 6) von bis zu 20 Mio. EUR und die Möglichkeit der Geltendmachung von immateriellem Schadenersatz (Art. 82) bei Verstößen gegen die DSGVO. Daneben können die Mitgliedstaaten weitere Strafbestimmungen vorsehen (Art. 84).[56]

Die Höhe der Strafe kann sich auch mit 2 bis 4 % des *„gesamten weltweit erzielten Jahresumsatzes*" bemessen. Was der Jahresumsatz eines nur für das jeweilige Verfahren eingerichtete Schiedsverfahren ist, ist unklar. Als potentielle Bemessungsgrundlagen kommt der Jahresverdienst des einzelnen Schiedsrichters oder des gesamten Schiedsgerichts (oder gar der dahinterstehenden Kanzleien) oder der Streitwert des Schiedsverfahrens in Betracht.

Kriterium für die Bemessung der Strafhöhe ist ua die Vorsätzlichkeit oder Fahrlässigkeit des Verstoßes (Art. 83 Abs. 1 lit. c). In der Anwendung der DSGVO allgemein und insbes. im Schiedsbereich besteht in etlichen Punkten rechtlicher Argumentationsspielraum. Um im Fall eines Datenschutzverstoßes darlegen zu können, dass das Schiedsgericht mit der notwendigen Sorgfalt gehandelt hat, sollte das Schiedsgericht im Datenschutz-Protokoll auch rechtliche Erwägungen dokumentieren, warum es eine bestimmte Maßnahme (nicht) getroffen hat.

2. Datenschutzverletzungen: Verletzung des *ordre public*?

Seit der grundlegenden EuGH-Entscheidung in *Eco Swiss v. Benetton*[57] steht fest, dass eine Verletzung einer Eingriffsnorm aus dem Europarecht eine Verletzung des (europäischen) *ordre public* darstellen kann.[58] Eine solche Verletzung begründet einen Aufhebungsgrund, sofern am Sitz des Schiedsgerichts die Verletzung des nationalen *ordre public* einen Aufhebungsgrund darstellt.[59] Die Frage ist daher: Handelt es sich bei den Vorschriften der DSGVO um Eingriffsnormen, deren Verletzung einen Aufhebungsgrund begründen kann?

Gemäß Art. 9 Abs. 1 Rom-I VO sind Eingriffsnormen zwingende Vorschriften, deren Einhaltung als so entscheidend für die Wahrung des öffentlichen Interesses angesehen wird, dass sie ungeachtet einer Rechtswahl oder Kollisionsnormen auf alle Sachverhalte anzuwenden sind, die in ihren Anwendungsbereich fallen.[60] Demgemäß handelt es sich wohl beim Großteil der Bestimmungen der DSGVO um Eingriffsnormen.

Allerdings betonte der EuGH in *Eco Swiss v. Benetton*, dass das dort anwendbare Kartellrecht und konkret der (damalige) Art. 85 EG-Vertrag eine grundlegende Bestimmung ist, *„die für die Erfüllung der Aufgaben der Gemeinschaft und insbesondere für das Funktionieren des Binnenmarktes unerläßlich ist.*"[61] Ob es sich bei den Bestimmungen der DSGVO um ähnlich grundlegende Bestimmungen handelt und ob deren Verletzung daher die Aufhebung eines Schiedsspruchs rechtfertigt, wird letztlich der EuGH zu klären haben.

Die Autoren sprechen sich aus folgenden Gründen gegen die undifferenzierte Qualifikation von Datenschutzverletzungen als Aufhebungsgrund aus.

Zunächst sollte nicht jede erdenkliche Datenschutzrechtsverletzung zur Aufhebung eines Schiedsspruchs führen können. Anderenfalls könnte bereits die irrtümliche Weiterleitung eines Schriftsatzes an einen Nichtbeteiligten einen Aufhebungsgrund darstellen. Ähnlich zur österreichischen Rechtsprechung zu Gehörsverletzungen[62] müssten die Verletzungen des Datenschutzrechts eine (noch zu bestimmende) Intensität erreichen, um als Aufhebungsgrund in Frage zu kommen.

Außerdem ist nicht ausschließlich das Schiedsgericht für die Wahrung des Datenschutzrechts der betroffenen Personen verantwortlich. Vor allem die Parteien und deren Vertreter verarbeiten während eines Schiedsverfahrens ebenfalls personenbezogene Daten in großem Umfang. Es könnte daher eine Guerilla-Taktik dahingehend ermöglicht werden, dass Parteien bewusst Datenschutzverletzungen begehen, um gleichzeitig einen Aufhebungsgrund für den Fall ihres Unterliegens zu setzen.

Es ist ferner zu berücksichtigen, dass jene betroffene Person, deren Recht auf Datenschutz verletzt wurde, in den meisten Fällen nicht Partei des Schiedsverfahrens ist. Es ist insofern wohl zu verneinen, dass den Parteien

> Cervenka/Schwarz: Datenschutz im Schiedsverfahren – die Rolle des Schiedsgerichts (SchiedsVZ 2020, 78) 85

dennoch eine Aufhebungsmöglichkeit eingeräumt werden soll.

Schließlich ist das Datenschutzrecht weder eindeutig dem materiellen noch dem verfahrensrechtlichen *ordre public* zuordenbar.

VII. Zusammenfassung

Aufgrund der besonderen Einflussmöglichkeit des Schiedsgerichts auf die Gestaltung des Verfahrens kommt ihm eine Schlüsselrolle bei der Schaffung eines Rahmens zum Schutz personenbezogener Daten im Schiedsverfahren zu. Zu diesem Zweck sollte es so früh als möglich gemeinsam mit den Parteien ein Datenschutz-Protokoll verfassen. Darin sind sämtliche datenschutzrechtlich relevanten Überlegungen anzuführen. Insbes. hat es den Zweck der Verarbeitung, deren Rechtsgrundlage und (bei einem Schiedsrichtersenat) die Vereinbarung zwischen den gemeinsam verantwortlichen Schiedsrichtern zu enthalten. Darüber hinaus sind darin Vorkehrungen für die Informationserteilung an die betroffenen Personen zu treffen, die technischen und organisatorischen Maßnahmen für die Schaffung

eines ausreichenden Datensicherheitsniveaus zu definieren, die datenschutzrechtlichen Modalitäten des Beweisverfahrens festzulegen und weitere Aspekte zu bestimmen und zu regeln.

Während des Schiedsverfahrens sollte das Schiedsgericht die Einhaltung des getroffenen Datenschutz-Protokolls durch sämtliche Beteiligten gewährleisten. Das Schiedsgericht hat dabei einerseits das datenschutzrechtsrelevante Verhalten der Beteiligten zu prüfen. Andererseits hat es Maßnahmen bei Missachtung datenschutzrechtlicher Bestimmungen zu ergreifen.[63]

Schließlich hat das Schiedsgericht auch beim Verfassen von prozessleitenden Verfügungen und letztlich auch des Schiedsspruchs im Sinne der Datenminimierung sicherzustellen, nur jene personenbezogenen Daten zu verarbeiten, die für deren Erlass tatsächlich notwendig sind.

---

1 Der Artikel gibt ausschließlich die persönliche Meinung der Autoren wieder. Die Autoren bedanken sich bei der DORDA Schiedsrechtspraxis unter *Veit Öhlberger* sowie dem DORDA Datenschutzrechtsteam unter *Axel Anderl* sowie *Felix Hörlsberger* und insbes. bei *Nino Tlapak*, *Dominik Schelling* sowie *Martin Platte* von PLATTE disputes.solutions für deren Anregungen und Unterstützung.

* MMag. Anja Cervenka ist Rechtsanwaltsanwärterin in der Schiedsrechtspraxis von DORDA Rechtsanwälte GmbH und Mag. Philipp Schwarz ist Rechtsanwaltsanwärter bei PLATTE disputes.solutions, beide in Wien.

2 VO (EU) 2016/679.

3 DIS FAQ Datenschutz für DIS-Schiedsverfahren, 9.8.2019; *ICC Note to Parties and Arbitral Tribunals on the Conduct of the Arbitration under the ICC Rules of Arbitration*, Rz. 80 ff.

4 Auszüge eines Entwurfs des Leitfadens wurden in den Parteienschriftsätzen im NAFTA-Verfahren *Tennant Energy, LLC v. Government of Canada*, PCA Case No. 2018-54 veröffentlicht.

5 Ohne Anspruch auf Vollständigkeit s. etwa *Rosenthal*, Complying with the General Data Protection Regulation (GDPR) in International Arbitration – Practical Guidance, ASA Bull. 2019/4, 822 (dieser Beitrag enthält Muster etwa eines Verarbeitungsprotokolls); *Fritz/Prantl/Leinwather/Hofer*, Datenschutz im internationalen Schiedsverfahren, SchiedsVZ 2019, 307; *Burianski/Braun*, DSGVO und internationale Schiedsverfahren – ein Jahr danach, BB 2019, 1096; *Zahariev*, Data Protection in Commercial Arbitration, 2019; *Paisley*, It's All About the Data: The Impact of the EU General Data Protection Regulation on International Arbitration, Fordham Int. L. J. 2018, 912; *Hay*, The Invisible Arm of GDPR in International Treaty Arbitration, Kluwer Arbitration Blog, 29.8.2019.

6 Dies gilt einfachgesetzlich auch in Österreich trotz des weiterhin bestehenden allgemeinen Grundrechts auf Datenschutz in § 1 DSG, s. hierzu *Anderl/Hörlsberger/Müller*, Kein einfachgesetzlicher Schutz für Daten juristischer Personen, ÖJZ 2018, 14.

7 Aus Gründen der Einfachheit in Folge als „Union" bezeichnet.

8 ErwGr 22 DSGVO. Im Detail s. hierzu, *European Data Protection Board*, *Guidelines 3/2018 on the territorial scope of the* GDPR (Art. 3), 12.11.2019. Nach einem Entwurf der *IBA-ICCA Task Force* könnten jedoch bereits Mietvereinbarungen eines Schiedsrichters außerhalb der EU mit einer Kammer innerhalb der EU ausreichend sein für die Anwendbarkeit der DSGVO (*IBA-ICCA Joint Task Force on Data Protection in International Arbitration*: *RoadMap to Data Protection in International Arbitration Explanatory Notes*, auszugsweise veröffentlicht in *Tennant Energy, LLC v. Government of Canada*, PCA Case No. 2018-5, *Investor's submission on confidentiatlity*, Rz. 22).

9 *Tennant Energy, LLC v. Government of Canada*, PCA Case No. 2018-54, *Tribunal's communication to the parties*, 24.6.2019. Zu weiteren Erwägungen in die-

sem Verfahren s. *Hay*, The Invisible Arm of GDPR in International Treaty Arbitration, Kluwer Arbitration Blog, 29.8.2019.

10 *Hay*, The Invisible Arm of GDPR in International Treaty Arbitration, Kluwer Arbitration Blog, 29.8.2019.

11 Vgl. *European Data Protection Board*, *Guidelines 3/2018 on the territorial scope of the* GDPR (Art. 3), 12.11.2019, 10.

12 EuGH C-131/12, Rz. 56; ebenso EuGH C-210/16, Rz. 60.

13 Im Detail s. hierzu *Fritz/Prantl/Leinwather/Hofer*, Datenschutz im internationalen Schiedsverfahren, SchiedsVZ 2019, 307.

14 Für Österreich: *Hausmaninger* in Fasching/Konecny, Zivilprozessgesetze, 3. Aufl., ZPO § 587 Rz. 123; für Deutschland: *Prütting*, Die rechtliche Stellung des Schiedsrichters, SchiedsVZ 2011, 235.

15 Zur Abgrenzung zwischen Auftragsverarbeiter und Verantwortlicher s. Artikel-29-Datenschutzgruppe, Stellungnahme 1/2010 zu den Begriffen *„für die Verarbeitung Verantwortlicher"* und *„Auftragsverarbeiter"* (WP 169). Wird die Kanzlei als Auftragsverarbeiter für den Schiedsrichter tätig, ist eine Auftragsverarbeitervereinbarung gemäß Art. 28 DSGVO abzuschließen.

16 EuGH C-210/16, Rz. 31 ff.

17 *Paisley*, It's All About the Data: The Impact of the EU General Data Protection Regulation on International Arbitration, Fordham Int. L. J. 2018, 912.

18 *ICC Note to Parties and Arbitral Tribunals on the Conduct of the Arbitration under the ICC Rules of Arbitration*, Rz. 84.

19 Vgl hierzu jedoch *Rosenthal*, Complying with the General Data Protection Regulation (GDPR) in International Arbitration – Practical Guidance, ASA Bull. 2019/4, 825, wonach sich bei gemeinsamen Verantwortlichen gemäß Art. 26 Abs. 3 die Anwendung der DSGVO auch auf Personen erstrecken würde, die nicht in den räumlichen Anwendungsbereich fallen.

20 *Rosenthal*, Complying with the General Data Protection Regulation (GDPR) in International Arbitration – Practical Guidance, ASA Bull. 2019/4, 825 ff.; DIS FAQ Datenschutz für DIS-Schiedsverfahren, 9.8.2019, 3 f.

21 DIS FAQ Datenschutz für DIS-Schiedsverfahren, 9.8.2019, 3 f.

22 S. hierzu *Fritz/Prantl/Leinwather/Hofer*, Datenschutz im internationalen Schiedsverfahren, SchiedsVZ 2019, 307.

23 EuGH C-210/16, Rz. 31 ff.

24 EuGH C-210/16, Rz. 43.

25 Die Einwilligung muss freiwillig, für einen bestimmten Zweck, eindeutig und auf informierter Grundlage erteilt werden; vgl. ErwGr 43 DSGVO; EuGH C-673/17, Rz. 52 ff.; *Kastelitz/Hötzendorfer/Tschohl* in Knyrim, DatKomm Art. 6 DSGVO, Rz. 20 ff.; *Reimer* in Sydow, DSGVO, 2. Aufl., Art. 6 Rz. 15 ff.; *Heberlein* in Ehmann/Selmayr, DS-GVO, 2 Aufl., Art. 6 Rz. 7 ff.; *Buchner/Petri* in Kühling/Buchner, Datenschutz-Grundverordnung/BDSG, 2. Aufl., Art. 6 Rz. 19 ff.; *Frenzel* in Paal/Pauly, Datenschutz-Grundverordnung Bundesdatenschutzgesetz, 2. Aufl., Art. 6 Rz. 11.

26 Art. 6 Abs. 1 lit. b DSGVO: *„die Verarbeitung ist für die Erfüllung eines Vertrages,* ***dessen Vertragspartei die betroffene Person ist****, […] erforderlich*" [Hervor. d. Verf.].

27 *Kastelitz/Hötzendorfer/Tschohl* in Knyrim, DatKomm, Art. 6 DSGVO Rz. 39.

28 Größenschluss aus Art. 9 Abs. 2 lit. f DSGVO; *Reimer* in Sydow, DSGVO, 2 Aufl., Art. 6 Rz. 55; *Kastelitz/Hötzendorfer/Tschohl* in Knyrim, DatKomm, Art. 6 DSGVO Rz. 54; vgl. Artikel-29-Datenschutzgruppe, Stellungnahme zum Begriff des berechtigten Interesses (WP 217) 31 f. (zu Art. 7 DS-RL).

29 *Haidinger* in Knyrim, DatKomm, Art. 21 DSGVO Rz. 41; *Helfrich* in Sydow, DSGVO, 2. Aufl., Art. 21 Rz. 68; *Martini* in Paal/Pauly, Datenschutz-Grundverordnung Bundesdatenschutzgesetz, 2. Aufl., Art. 21 Rz. 41 ff.

30 Art. 21 Abs. 1 DSGVO verwendet den Begriff *„dienen"* und weicht daher augenscheinlich vom in Art. 6 DSGVO verankerten Erforderlichkeitsgrundsatz ab, s. dazu *Kamann/Braun* in Ehmann/Selmayr, DS-GVO Datenschutz-Grundverordnung, 2. Aufl. Art. 21 Rz. 29; *Haidinger* in Knyrim, DatKomm Art. 21 DSGVO Rz. 41.

31 *Haidinger* in Knyrim, DatKomm, Art. 21 DSGVO Rz. 40 ff.

32 S. auch ErwGr 20.
33 S. hierzu etwa *Peuker* in Sydow, DSGVO, 2. Aufl., Art. 23 Rz. 31, wonach Gerichtsverfahren iSd Art. 23 Abs. 1 lit. f DSGVO alle Verfahren umfasst „*an deren Ende eine bindende, auf Recht gestützte Entscheidung durch einen unabhängigen Spruchkörper steht, was in Deutschland auch Verfahren der freiwilligen Gerichtsbarkeit einschließe*." Bei der Ausnahme des Art. 23 Abs. 1 lit. j DSGVO ist fraglich, ob dies nur die Parteien bei Durchsetzung ihrer Ansprüche oder das Schiedsgericht als Spruchkörper betrifft. Jedenfalls sind davon außergerichtliche Verfahren erfasst, s. hierzu *Fritz/Prantl/Leinwather/Hofer*, Datenschutz in internationalen Schiedsverfahren, SchiedsVZ 2019, 304 mwN.
34 Die englische Datenschutzbehörde hat offensichtlich eine Ausnahme für Schiedsverfahren parallel zu jener für Gerichtsverfahren auf Anfrage der LCIA ausdrücklich abgelehnt, s. hierzu *Tennant Energy, LLC v. Government of Canada*, PCA Case No. 2018-5, *Investor's submission on confidentiatlity*, Rz. 24.
35 S. hierzu im Detail DIS FAQ Datenschutz für DIS-Schiedsverfahren, 9.8.2019, 7.
36 *Libananco v*. *Republic of Turkey*, ICSID Case No. ARB/06/8; *Opic Karimum Corporation v. Venezuela*, ICSID Case No. ARB/10/14; *Kılıç v. Turkmenistan*, ICSID Case No. ARB/10/1; *Caratube International Oil Company and MrDevincci Saleh Hourani v*. *Kazakhstan*, ICSID Case No. ARB/13/13.
37 S. etwa *Debevoise & Plimpton, Protocol to Promote Cybersecurity in International Arbitration*, https://www.debevoise.com/~/media/files/capabilities/cybersecurity/protocol_cybersecurity_intl_arb_july2017.pdf (dieser Link und alle weiteren Links zuletzt abgerufen am 29.1.2020).
38 *Protocol on Cybersecurity in International Arbitration* (*2020 Edition*), https://www.arbitration-icca.org/media/14/76788479244143/icca-nyc_bar-cpr_cybersecurity_protocol_for_international_arbitration_-_print_version.pdf.
39 *Martini* in Paal/Pauly, Datenschutz-Grundverordnung Bundesdatenschutzgesetz, 2. Aufl., Art. 32 Rz. 35 ff.; *Jandt* in Kühling/Buchner, Datenschutz-Grundverordnung/BDSG, 2. Aufl., Art. 32 Rz. 22 ff.; *Pollirer* in Knyrim, DatKomm Art. 32 DSG-VO Rz. 38.
40 *Martini* in Paal/Pauly, Datenschutz-Grundverordnung Bundesdatenschutzgesetz, 2. Aufl., Art. 32 Rz. 35 ff.; *Jandt* in Kühling/Buchner, Datenschutz-Grundverordnung/BDSG, 2. Aufl., Art. 32 Rz. 22 ff.; *Pollirer* in Knyrim, DatKomm Art. 32 DSG-VO Rz. 39.
41 *Martini* in Paal/Pauly, Datenschutz-Grundverordnung Bundesdatenschutzgesetz, 2. Aufl., Art. 32 Rz. 35 ff.; *Jandt* in Kühling/Buchner, Datenschutz-Grundverordnung/BDSG, 2. Aufl., Art. 32 Rz. 22 ff.; *Pollirer* in Knyrim, DatKomm Art. 32 DSG-VO Rz. 40.
42 *Pollirer* in Knyrim, DatKomm Art. 32 DSGVO Rz. 41.
43 *Duarte*, Essential Tips on Cybersecurity for Arbitrators: Identify, Protect, Detect, Respond and Recover, Kluwer Arbitration Blog 6.2.2019.
44 *Protocol on Cybersecurity in International Arbitration* (*2020 Edition*), Principle 9.
45 *Duarte,* Essential Tips on Cybersecurity for Arbitrators: Identify, Protect, Detect, Respond and Recover, Kluwer Arbitration Blog 6.2.2019.
46 Die *ICC Commission* hat einen Report zur Benutzung von Informationstechnologien herausgegeben: *ICC Commision Report, Information Technology in International Arbitration*.
47 *Protocol on Cybersecurity in International Arbitration* (*2020 Edition*), Principle 9.
48 *Protocol on Cybersecurity in International Arbitration* (*2020 Edition*), Principles 11, 12.
49 Vgl. Art. 32 Abs. 1 DSGVO; vgl. *Protocol on Cybersecurity in International Arbitration* (*2020 Edition*), Principle 6: „*the burden, costs, and the relative resources of the parties, arbitrators, and any administering institution*."
50 S. https://sccinstitute.com/scc-platform/.
51 *Paisley*, It's All About the Data: The Impact of the EU General Data Protection Regulation on International Arbitration, Fordham Int. L. J. 2018, 914.
52 S. Art. 23 ICC-Schiedsgerichtsordnung.
53

Art. 4 Regeln über die effiziente Durchführung internationaler Schiedsverfahren (Prager Regeln); s. auch *Burianski/Braun*, DSGVO und internationale Schiedsverfahren – ein Jahr danach, BB 2019, 1100.

54 S. hierzu *Rosenthal*, Complying with the General Data Protection Regulation (GDPR) in International Arbitration – Practical Guidance, ASA Bull. 2019/4, 829 ff.

55 Etwa bei Nutzung der Kanzleiinfrastruktur, Beiziehung von Übersetzern und *court reporter*.

56 Für Deutschland s. §§ 41 ff. BDSG; für Österreich s. §§ 62 f. DSG.

57 EuGH C-126/97.

58 EuGH C-126/97, Rz. 39.

59 EuGH C-126/97, Rz. 41.

60 S. zum Begriff der Eingriffsnorm auch *Horn*, Zwingendes Recht in der internationalen Schiedsgerichtsbarkeit, SchiedsVZ 2008, 210.

61 EuGH C-126/97, Rz. 36.

62 Vgl. RIS-Justiz, RS0045092 wonach nur der völlige Gehörsentzug zur Aufhebung berechtigt. Diese Rechtsprechung zur Gehörsverletzung steht zurecht unter Kritik der Lehre.

63 Das Schiedsgericht könnte bspw. Parteien datenschutzrechtskonformes Verhalten bei Androhung von Kostenfolgen auftragen.