EUROPA-UNIVERSITÄT
VIADRINA
FRANKFURT (ODER)

Band 29

Viadrina-Schriftenreihe zu Mediation und Konfliktmanagement

Annette Ehrnsperger

Vertraulichkeit und Datenschutz bei der Online-Mediation über Videokonferenzen

Wolfgang Metzner Verlag

Band 29

Viadrina-Schriftenreihe zu Mediation und Konfliktmanagement

Band 29

Viadrina-Schriftenreihe zu Mediation und Konfliktmanagement

Herausgegeben von
Prof. Dr. Ulla Gläßer, LL. M.
Dipl.-Psych. Kirsten Schroeter
Dr. Felix Wendenburg, M. B. A.

Annette Ehrnsperger

Vertraulichkeit und Datenschutz bei der Online-Mediation über Videokonferenzen

Wolfgang Metzner Verlag

Master-Studiengang Mediation
und Konfliktmanagement
Masterarbeit
Studiengang 2019/2021

EUROPA-UNIVERSITÄT
VIADRINA
FRANKFURT (ODER)

© Wolfgang Metzner Verlag, Frankfurt am Main 2021

Das Werk ist urheberrechtlich geschützt.
Jede Verwertung außerhalb der Freigrenzen des Urheberrechts ist ohne Zustimmung des Verlags unzulässig und strafbar. Das gilt insbesondere für Vervielfältigungen, Übersetzungen, Mikroverfilmungen und die Einspeicherung und Verarbeitung in elektronischen Systemen.

Printed in Germany
ISBN 978-3-96117-095-1 (Print)
ISBN 978-3-96117-096-8 (Online)
ISSN 2365-4155

Bibliografische Information der Deutschen Bibliothek
Die Deutsche Bibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Um sich auseinander zu setzen, muss man sich erstmal zusammensetzen.

Erhard Horst Bellermann
(*1937), deutscher Bauingenieur, Dichter und Aphoristiker
Quelle: Bellermann, Schmetterlinge im Kopf. Gedanken in Reim und Prosa, 2006.

Inhalt

Vorwort

Dieses Buch ist eine überarbeitete und aktualisierte Fassung meiner Masterarbeit, die ich im 11. Studiengang Mediation und Konfliktmanagement (2019–2021) an der Europa-Universität Viadrina in Frankfurt (Oder) angefertigt und im November 2020 eingereicht habe. Zum Zweck der Veröffentlichung habe ich sie aktualisiert und um einige weiterführende Gedanken ergänzt.

Die Arbeit widmet sich aktuellen Fragen der Vertraulichkeit sowie des Datenschutzrechts bei Mediationen, die über Videokonferenzen durchgeführt werden. Betrachtet werden dabei sowohl die Auswahl des Anbieters als auch der Einsatz des Konferenzdienstes selbst. In der Folge des EuGH Urteils Schrems II vom Juli 2020 haben sich eine Vielzahl von datenschutzrechtlichen Herausforderungen ergeben, die in der Praxis zu großer Unsicherheit führen. Vorliegend werden das geltende Recht und die zugrundeliegenden Interessen beleuchtet und darauf aufbauend eine Einschätzung für den praktischen Umgang mit den aktuellen Rechtsfragen gegeben.

Mein Dank gebührt allen voran meinem Dozenten Dr. Felix Wendenburg, mit dem ich erste Ideen zur Themenfindung austauschen konnte, der Betreuerin meiner Masterarbeit, Frau Pia Mahlstedt, die mich bei der Schärfung der Fragestellung und der Strukturierung zielführend unterstützt hat, und dem Zweitgutachter, Herrn Dr. Christof Berlin, der mein Interesse an einer Veröffentlichung geweckt hat.

Zudem gilt mein Dank den Verantwortlichen des Master-Studiengangs Mediation und Konfliktmanagement Prof. Dr. Ulla Gläßer LL.M., Dipl.-Psych. Kirsten Schroeter, Dr. Felix Wendenburg M.B.A. und Dipl.-Psych. Nicole Becker M.A. für die Aufnahme dieser Masterarbeit in die Viadrina-Schriftenreihe zu Mediation und Konfliktmanagement.

Meinen Teamkolleg:innen habe ich dafür zu danken, dass sie mir den Rücken freigehalten haben, und meiner Chefin dafür, dass sie mein Vorhaben jederzeit unterstützt und mir die notwendigen Freiräume zugestanden hat.

Schließlich möchte ich meinem Ehemann, Dr. Markus Ehrnsperger, und unseren drei Kindern Arved, Jördis und Gerald dafür Danke sagen, dass sie mich während der Zeit der Mehrfachbelastung durch Studium neben dem Job und dann durch COVID-19 bedingtes „Alle sind jetzt von morgens bis abends zu Hause“ mit Geduld und Liebe unterstützt und ertragen haben.

Dr. Annette Ehrnsperger, Mai 2021

Abstract – Confidentiality and Data Protection in Mediation via Video Conferencing

This legal thesis examines the special requirements that arise from the confidentiality principle in mediation law and from data protection law when using video conferences for mediation purposes.

The thesis analyses the applicable law and its foundation in Human Rights legislation, taking into account the interests of the individuals, both during the actual conference as well as in the consideration of the legal basis.

Particular challenges arise when using video conferencing providers who either run their conferencing infrastructure not only in the EEA, but on globally distributed servers, especially in the USA, or administrate regional European data centers from outside the EEA. They may be subject to local law which is not compliant with European data protection law. It is precisely here that future EU foreign policy will make a major contribution to the evolution and harmonization of the currently contradictory legal systems. Since technology is also constantly evolving, there is hope that a solution will be found that is equally viable for the individuals' fundamental rights and for the general interest.

At present, the mediator should be aware of the uncertainty and choose and run the selected video conferencing service with due care. The annexes provide a list of practical things to remember in the context of videoconferencing, a particular data protection checklist for the choice of the provider and a draft for a data protection information document. They may be useful for evaluating the offers from different providers as well as using videoconferencing in mediative practice.

1. Einleitung

Muss man sich wirklich physisch zusammensetzen, um eine Auseinandersetzung zu führen? Gerade angesichts der derzeitigen pandemiebedingten Abstandsgebote aber auch allgemein im Zuge der zunehmenden Digitalisierung ist eine Zunahme von mediativen Konfliktlösungen auch bei nur „virtueller" gleichzeitiger Anwesenheit der Beteiligten zu beobachten.

Der Einsatz moderner Kommunikationsmittel birgt Chancen für die Mediation (Abschnitt 2), geht aber auch mit neuen Risiken insbesondere für die Vertraulichkeit der Mediation sowie in Bezug auf Datenschutzrecht einher. Sowohl bei der Auswahl eines geeigneten Konferenzdienstes als auch bei dessen Einsatz stellen sich eine Vielzahl tatsächlicher und rechtlicher Herausforderungen. Gerade das Datenschutzrecht hat bei der videokonferenzgestützten Durchführung der Mediation im Vergleich zur Mediation vor Ort einen viel größeren Stellenwert.

Bei der Klärung der rechtlichen Grundlagen (Abschnitte 3 und 4) wird auf die jeweils zugrundeliegenden Interessen einzugehen sein. Sie haben maßgeblichen Einfluss auf die konkrete Ausprägung der Pflichten aller Beteiligten in der Praxis in Bezug auf Vertraulichkeit und Datenschutz haben.

Die kurze Darstellung der Vertragskonstellation im Dreieck zwischen den Medianden, dem Mediator[1] und den Dienstanbietern (Abschnitt 5) bildet die Basis für die anschließende Untersuchung der videokonferenzspezifischen Fragen in Bezug auf Vertraulichkeitspflichten (Abschnitt 6) und Datenschutzrecht (Abschnitt 7). Dort haben sich insbesondere beim Einsatz internationaler Dienstanbieter infolge der jüngsten EuGH-Enscheidung „Schrems II" besondere Fragestellungen ergeben.

In Abschnitt 8 folgen abschließende Empfehlungen. In den Anhängen befinden sich eine Checkliste für die Auswahl des geeigneten Dienstes, eine Sammlung von Praktischen Hinweisen sowie ein Muster für eine Datenschutzerklärung für die Medianden und schließlich eine Liste der Quellen der untersuchten Auftragsverarbeitungsvereinbarungen.

[1] Im Folgenden wird aus Gründen der leichteren Lesbarkeit auf die gleichzeitige Verwendung der männlichen und weiblichen Sprachformen bzw. andere genderneutrale Darstellungen verzichtet und das generische Maskulinum verwendet. Sämtliche Personenbezeichnungen gelten gleichermaßen für alle Geschlechter.

2. Online-Mediation über Videokonferenzen

Zu Beginn dieser Arbeit möchte ich nach der erforderlichen Begriffsklärung auf das Wesen der sog. „Online-Mediation“ und die Interessenlage der Beteiligten bei der Durchführung des Mediationsverfahrens im Wege einer Videokonferenz eingehen.

2.1. Begriffsklärung

Die Begriffe „remote“ und „online“ werden im Kontext der Mediation für Fälle verwendet, in denen im weitesten Sinne keine gleichzeitige körperliche Anwesenheit der Teilnehmer und des Mediators gegeben ist[2] bzw. – spezieller, dafür technisch unschärfer formuliert – in denen die Mediation „über das Internet oder andere Kommunikationsmedien“ durchgeführt wird[3]. Nicht ausreichend ist, wenn lediglich computergenerierte Abstimmungs- oder Visualisierungshilfsmittel wie „Heatmaps“ oder online bereitgestellte „Voting-Tools“ für Abstimmungen eingesetzt werden[4]. Durch den technischen Fortschritt, aber auch durch äußere Umstände, wie die sich seit dem Frühjahr 2020 weltweit ausbreitende COVID-19 Pandemie[5], haben Videokonferenzen Eingang in den Alltag der Menschen und damit auch in die Konfliktbearbeitung gefunden.

Wir bewegen uns zwar noch nicht in der vor ca. 20 Jahren in Aussicht gestellten Welt, in der „Avatare komplexe Fälle halbautomatisch mediieren“[6], indem sie softwaregestützt paraphrasieren „wie jeder gute Mediator“ und mittels Machine-Learning-Eigenschaften in der Lage sind, aus Rückmeldungen der Medianden zu lernen. Die Technik und auch die Gewöhnung der Nutzer an virtuelle Kommunikationsmethoden haben sich jedoch wesentlich weiterentwickelt. Videokonferenzen stellen inzwischen – anders als in früheren Abhandlungen zur „Online-Mediation“[7] – den Schwerpunkt der Betrachtungen dar[8]. Die in Reaktion auf die COVID-19-Pandemie ausgesprochenen Kontaktbeschränkungen haben in vielen Ländern den Ersatz per-

---

[2] So z. B. Haft/Schlieffen-*Lapp,* § 23 Rn. 1.
[3] So Rickert KD 2019, 64, 64.
[4] So jedoch Wacker ZKM 2001, 265, 267.
[5] Gläßer/Sinemillioglu/Wendenburg ZKM 2020, 80, 80.
[6] So die Vision von Wacker ZKM 2001, 265, 268f.
[7] Wacker ZKM 2001, 265, 267f.; Fietkau/Renz/Trénel ZKM 2001, 132, 135; Loock-Wagner ZKM 2002, 206, 209.
[8] So bereits Rickert ZKM 2009, 168ff. und auch Gläßer/Sinemillioglu/Wendenburg ZKM 2020, 80, 80.

sönlicher Arbeitstreffen durch Videokonferenzen zusätzlich befördert. Auch Mediatoren greifen inzwischen regelmäßig auf diese Technik zurück. Niederschwellige, oft kostenlose Angebote lokaler aber auch internationaler Dienstanbieter machen Videokonferenzen schnell verfügbar. Wie sieht eine typische Mediation über Videokonferenz daher aus, und welche Interessen der Beteiligten sind dabei prägend?

2.2. Typisches Format

Das typische Format der videokonferenzbasierten Mediation lässt sich wie folgt beschreiben[9]:

Der Mediator hat den zu verwendenden Videokonferenzdienst mit den Beteiligten abgestimmt, einen Termin aufgesetzt und den Parteien jeweils die Einwahldaten geschickt. Die Beteiligten sind an ihrem Arbeitsplatz oder zu Hause und nutzen einen PC mit Webcamera (i. d. R. einen Laptop mit integrierter Kamera), oder ein Smartphone, jeweils mit Internetanschluss. Auf den Endgeräten ist die erforderliche Konferenzanwendung installiert, oder die Teilnahme erfolgt direkt über den Webbrowser[10]. Der Mediator eröffnet die Konferenz zur vereinbarten Zeit, und die Beteiligten wählen sich ein. Die Beteiligten kommunizieren über die Audio- und Videoverbindung, d. h. sie hören und sehen einander. Die Bildschirmansicht hängt von der verwendeten Software und der gewählten Einstellung ab, lässt sich aber allgemein wie folgt beschreiben: Auf dem Bildschirm sind in mehreren Fenstern die Namensliste der Teilnehmer, die Videos der Parteien und des Mediators und ggf. ein Chat für Textnachrichten und / oder eine gemeinsame Präsentations- oder Arbeitsfläche zu sehen.

2.3. Interessenlage bei der Mediation über Videokonferenz

Auch außerhalb der durch COVID-19 bedingten Sondersituation entscheiden sich Beteiligte aus unterschiedlichen Gründen für die Durchführung der Mediation in

[9] So bereits Rickert ZKM 2009, 169 und Gläßer/Sinemillioglu/Wendenburg ZKM 2020, 81ff.

[10] Siehe auch die detaillierte Beschreibung im BSI Kompendium VK 4-2020, S. 31. Andere Videokonferenztechniken, insbesondere hardwarebasierte Lösungen mit speziellen Endgeräten werden hier ausgeklammert.

einem Online-Format, das nicht die physische Anwesenheit aller Beteiligten erfordert. Die Durchführung geht allerdings auch mit Risiken und Ambivalenzen einher[11]. Ein Blick auf die Motive und Interessen der Beteiligten erscheint daher sinnvoll:

Für alle Beteiligten bietet die Online-Durchführung primär einen Effizienzgewinn: Die **Überbrückung der räumlichen Entfernung**[12] sowie die Einsparung von zeitlichen und finanziellen Aufwänden insbesondere für Reise und Raummiete werden als positiv angesehen[13]. Das virtuelle Hinzuziehen eines Co-Mediators, der eigene Kompetenzen oder Perspektiven in die Sitzung einbringt[14], wird erleichtert. Möglichkeiten der Sitzungsunterbrechung, das Einrichten von „Break-Out-Sessions" für die interne **Parteiberatung oder Einzelgespräche**, sowie das Zuschalten von unterstützenden Dritten machen das Verfahren flexibler und erlauben ein passgenaues Eingehen auf konkrete Bedürfnisse und Konfliktgestaltungen[15]. Dem **Sicherheitsbedürfnis** der Parteien kann insbesondere in eskalierten Konflikten dadurch Rechnung getragen werden, dass der physische Kontakt vermieden und eine größere Distanz gewahrt wird[16]. Der niederschwellige Zugang zur Mediation erhöht die Verhandlungsbereitschaft und stärkt die Autonomie der Parteien[17].

Videokonferenzen sind für die Medianden ein wichtiges Mittel um Verständnis zu fördern, denn sie erlauben eine größere **Reichhaltigkeit der Kommunikation**[18]: Bei rein textlicher Kommunikation wird nur der Sachinhalt übermittelt (verbale Kommunikation)[19]. Bei Telefonie werden bereits Sprachsignale übertragen, d. h. neben der Sachinformation erhält der Zuhörer zumindest auch über Tonlagen, Stimmführung und Sprachmelodie[20] bestimmte Informationen über die emotionale

---

[11] Siehe hierzu die Zusammenstellungen bei Gläßer/Sinemillioglu/Wendenburg ZKM 2020, 133, 134f. und Schwitteck/von Baumbach, ZKM 2020, 104ff., sowie Haft/Schlieffen-*Lapp,* § 23 Rn. 5.

[12] Siehe auch die praktischen Beispiele von Schwittek/von Baumbach-*Schwittek*, S. 106, sowie Hinterhölzl-Widi, S. 39 und Lütkehaus ZKM 2020, 102ff.

[13] Gläßer/Sinemillioglu/Wendenburg ZKM 2020, 133, 134.

[14] Hinterhölzl-Widi, S. 57.

[15] Gläßer/Sinemillioglu/Wendenburg ZKM 2020, 133, 134.

[16] Gläßer/Sinemillioglu/Wendenburg ZKM 2020, 133, 135 für hoch-eskalierte Konflikte; anders die empirischen Erfahrungen bei Hinterhölzl-Widi, S. 56f.

[17] Gläßer/Sinemillioglu/Wendenburg ZKM 2020, 133, 134.

[18] Siehe Kilburg Komet Blog 14.07.2020.

[19] Haft/Schlieffen-*Duss-von Werdt*, § 10 Rn. 40.

[20] Haft/Schlieffen-*Lapp*, § 23 Rn. 9 und Haft/Schlieffen-*Duss-von Werdt*, § 10 Rn. 40f.

Lage und über die Wichtigkeit des Gesagten für den Sprecher. Bei Videoübertragungen sind schließlich auch Mimik und bestenfalls Gestik des Sprechenden erkennbar. Diese Körpersprache übermittelt weitaus mehr Kanäle non-verbaler Kommunikation und hilft dem Zuhörenden, Verständnis für den Sprechenden zu entwickeln[21].

Das Interesse der Beteiligten an einer gleichberechtigten Teilnahme am Verfahren kann jedoch durch in unterschiedlichem Maß vorhandene **technische Ausstattung** oder auch persönliche Technikaffinität beeinträchtigt sein[22]: Technische Störungen aber auch Vorbehalte gegenüber internetbasierter Mediation können bei den Parteien ein Gefühl des Kontrollverlusts erzeugen, das letztlich die Autonomie beeinträchtigt. Die eingangs beschriebenen Effizienzgewinne können zudem durch schnelleres Ermüden während der Videokonferenz verringert werden[23]. Ebenso können die als vorteilhaft aufgeführte Distanz und der fehlende direkte Augenkontakt der Parteien zueinander und zum Mediator dazu führen, dass die Kommunikation an Authentizität verliert und nicht die für ein gegenseitiges Verständnis der Interessen erforderliche emotionale Nähe aufkommt[24].

Zur wirksamen Konfliktbearbeitung müssen solche Defizite durch **geeignete Vorgehensweisen kompensiert** werden: Der Mediator kann im Vorfeld bei der technischen Umsetzung Hinweise geben und Anleitungen zur Verfügung stellen, oder auch ein Konferenztool auswählen, das ggf. funktionsärmer, dafür aber leichter zugänglich ist. Vorbehalte der Parteien können durch Aufklärung abgebaut werden[25]. Während der Mediation können gezielte Pausen der Ermüdung, die in Anlehnung an den Videokonferenzdienst Zoom auch „Zoom Fatigue“[26] genannt wird, vorbeugen[27]. Dadurch, dass der Mediator selbst bei seiner eigenen Kommunikation auf Blickkontakt achtet und die Parteien direkt anspricht, hilft er ihnen ihre Aufmerksamkeit zu erhalten. Auch technische Einstellungen, wie z. B. das automatische Vergrößern des Videobildes des jeweils Sprechenden, kann durch die Größe der Videodarstellung mangelnde non-verbale Reichhaltigkeit der Kommunikation verringern und mehr Nähe bewirken[28].

---

[21] Haft/Schlieffen-*Duss-von Werdt*, § 10 Rn. 42.
[22] Haft/Schlieffen-*Lapp,* § 23 Rn. 11.
[23] Gläßer/Sinemillioglu/Wendenburg ZKM 2020, 80, 83.
[24] Gläßer/Sinemillioglu/Wendenburg ZKM 2020, 133, 135.
[25] Gläßer/Sinemillioglu/Wendenburg ZKM 2020, 80, 82f.
[26] Heim Blog 24.07.2020.
[27] Gläßer/Sinemillioglu/Wendenburg ZKM 2020, 80, 83 und Gläßer/Sinemillioglu/Wendenburg ZKM 2020, 133, 135.
[28] Gläßer/Sinemillioglu/Wendenburg ZKM 2020, 80, 84.

Die Interessenlage der Beteiligten und die Möglichkeiten ihr Rechnung zu tragen sind bei der Online-Mediation durch Videokonferenzen sehr vielgestaltig und fordern die Kreativität des Mediators und der Parteien heraus.

Um die Risiken die videokonferenzgestützten Online-Mediation insbesondere für Vertraulichkeit und Datenschutz und ihre mögliche Mitigation zu beschreiben, werden nun im Folgenden die rechtlichen Grundlagen und die ihnen zugrundeliegenden Interessen dargestellt.

3. Vertraulichkeit in der Mediation

Mediationsverfahren sind gemäß § 1 Abs. 1 MediationsG grundsätzlich vertraulich. Bereits die zugrundeliegende Europäische Mediations-Richtlinie[29] (Mediations-RL) benennt die Vertraulichkeit als *wichtig* für die Durchführung des Mediationsverfahrens[30], gibt den Mitgliedsstaaten dann allerdings in ihrem Art 7 Abs. 1 nur als Mindestvoraussetzung auf, diese durch eine entsprechende Anpassung der zivil- und handelsprozessrechtlichen Regelungen als Zeugnisverweigerungsrecht umzusetzen.

Der deutsche Gesetzgeber hat sich bei der Schaffung des Mediationsgesetzes entschieden, die Vertraulichkeit in Abweichung zu Art 3 lit. a Mediations-RL als Wesensmerkmal in die Definition des Mediationsverfahrens aufzunehmen. Sie ist jedoch abdingbar durch einvernehmliche Vereinbarung zwischen den Parteien, d. h. sie ist nicht konstitutiv[31].

Die Vertraulichkeitsmaxime enthält drei Elemente[32]: den Ausschluss der Öffentlichkeit, die Verschwiegenheitspflicht des Mediators und die Vertraulichkeitspflichten der Parteien untereinander[33].

3.1. Nichtöffentlichkeit

Anders als in Verfahren der staatlichen Gerichtsbarkeit, die gemäß § 169 S. 1 GVG der Allgemeinheit grundsätzlich zugänglich sein müssen, ist in Mediationsverfahren die Öffentlichkeit grundsätzlich ausgeschlossen. Dies ergibt sich aus einem Umkehrschluss zu § 2 Abs. 4 MediationsG[34]: Die Öffentlichkeit steht zur Disposition

---

[29] Richtlinie 2008/52/EG des Europäischen Parlaments und des Rates vom 21. Mai 2008 über bestimmte Aspekte der Mediation in Zivil- und Handelssachen, in den verschiedenen Sprachen abrufbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=celex%3A32008L0052.

[30] Siehe EG 23 zur Mediations-RL.

[31] Klowait/Gläßer-*Hagel* § 1 Rn. 6f und 9; Greger/Unberath/Steffek-*Greger* MediationsG § 1 Rn. 53.

[32] Wagner ZKM 2011, 164, 164 und Klowait/Gläßer-*Hagel* § 1 Rn. 7 teilen sie hingegen nur in zwei Bestandteile auf, indem sie die hier getrennt behandelten Elemente der Verschwiegenheitspflicht des Mediators und der Vertraulichkeit der Parteien untereinander übergreifend behandeln.

[33] So auch Weigel NJOZ 2015, 41, 42ff.

[34] Weigel NJOZ 2015, 41, 42.

der Parteien, und Dritte werden im Mediationsverfahren nur ausnahmsweise zugelassen, soweit die Parteien deren Teilnahme, als weitere Konfliktbeteiligte, Rechtsberater oder Experten einvernehmlich im Arbeitsbündnis[35] vereinbaren[36].

Welche Parteiinteressen stehen hinter diesem Element des Vertraulichkeitsgrundsatzes?

Im Gegensatz zur Mediation sind Gerichtsverfahren eine Ausprägung des staatlichen Gewaltmonopols, das auch in der Form der dritten Gewalt der Kontrolle der Allgemeinheit unterliegen muss[37]. Der Verfahrensgrundsatz der Öffentlichkeit ist Ausfluss der Prinzipien demokratischer Rechtspflege[38] und des Rechtsstaatlichkeitsgebots[39]. Da er somit nicht ausschließlich dem Schutz privater Interessen dient[40], kann er nicht gemäß § 295 Abs. 2 ZPO durch den Verzicht seitens der Parteien abbedungen werden[41]. Parteien, die eine gerichtliche Klärung ihres Rechtsstreits wünschen, sind daher an einer für die Allgemeinheit nachvollziehbaren, rechtssetzenden Entscheidung ihres Konfliktes durch einen legitimierten Dritten interessiert.

In der Mediation streben die Parteien dagegen eine eigenverantwortliche Konfliktlösung im Sinne der Privatautonomie an. Mit dem Ausschluss der Öffentlichkeit möchten die Streitenden nicht nur ihre Privatsphäre oder auch ihre Geschäftsgeheimnisse schützen[42] und selbst vor der öffentlichen Bloßstellung durch negative Presseberichterstattung[43] oder der Verwendung der Informationen durch Wettbewerber bewahrt werden[44]. Die Vertraulichkeit ihrer Gespräche ist vielmehr wesentlich für den Erfolg des Mediationsverfahrens[45]: Die Parteien wünschen sich in der Mediation einen geschützten Raum[46], der ihnen einen Informationsaustausch zur

---

[35] Haft/Schlieffen-*Kessen/Troja* § 14 Rn. 18 und Troja ZKM 2009, 152, 153.

[36] Siehe die Gesetzesbegründung in BT-Drs 17/5335, Teil B, zu § 1, S. 13. Eine öffentliche Mediation im berechtigten Allgemeininteresse kommt ggf. ausnahmsweise im Kontext öffentlicher Planungsvorhaben in Betracht, siehe Haft/Schlieffen-*Hartmann* § 28 Rn. 7 u. Greger/Unberath/Steffek-*Greger* MediationsG § 4 Rn. 3.

[37] Von Lewinski IDR 2003, 150, 153.

[38] Zöller ZPO-*Lückemann* § 169 GVG Rn. 1.

[39] MüKo ZPO-*Prütting* § 295 Rn. 16.

[40] Zu diesem Kriterium siehe MüKo ZPO-*Prütting* § 295 Rn. 6.

[41] Zöller ZPO-*Lückemann* § 169 GVG Rn. 15.

[42] Von Lewinski IDR 2003, 150, 153.

[43] Weigel NJOZ 2015, 41, 42.

[44] Von Lewinski IDR 2003, 150, 153.

[45] MüKo ZPO-*Ulrici* Anh. 1 zu § 278a MediationsG §§ 1–9 Rn. 44.

[46] Weigel NJOZ 2015, 41, 42.

Ergründung authentischer Konfliktursachen und Motive ermöglicht[47], damit durch Perspektivwechsel gegenseitiges Verständnis und Empathie gefördert werden[48]. Die Nichtöffentlichkeit unterstützt schließlich die Parteien in ihrer Suche nach gemeinsamen Einigungsoptionen[49], indem sie vor Polarisierung durch strategische „Litigation-PR" bewahrt[50].

Die vom Gesetzgeber hierzu gelieferte Begründung weist ausdrücklich darauf hin, dass der Erfolg der Mediation vom geschützten Rahmen der vertraulichen Mediation abhängt, in dem die Parteien zu einer gemeinsamen Basis für eine Lösung ihres Konflikts gelangen, die dann allerseits als gerecht wahrgenommen wird[51]. Dies entspricht der zukunftsgerichteten Lösungsorientierung der Mediation.

3.2. Verschwiegenheitspflicht des Mediators

Ein weiteres Element der Vertraulichkeit der Mediation ist die Pflicht des Mediators und seiner Hilfspersonen zur Verschwiegenheit gem. § 4 S. 1 und 2 MediationsG.

Hiernach sind der Mediator und seine Hilfspersonen dazu verpflichtet, das ihnen durch die Ausübung ihrer Tätigkeit bekannt Gewordene vertraulich zu behandeln. Hiervon umfasst sind nicht nur während des Mediationsverfahrens erlangte Kenntnisse über Tatsachen, Meinungsäußerungen, Emotionen oder Motive[52], sondern auch Informationen aus der Anbahnung des Verfahrens, d. h. auch die Namen der Parteien und die Tatsache, dass überhaupt eine Mediation durchgeführt wird[53]. Ausnahmen ergeben sich aus dem Ordre Public Vorbehalt in S. 3 derselben Vorschrift, sowie durch den Vorbehalt abweichender gesetzlicher Regelung in § 4 S. 1 MediationsG, insbesondere aus dem Anwendungsbereich des § 138 StGB, nach dem für

---

[47] MüKo ZPO-*Ulrici* Anh. 1 zu § 278a. MediationsG §§ 1–9 Rn. 44.
[48] Weigel NJOZ 2015, 41, 42.
[49] Wagner ZKM 2011, 164, 164.
[50] Weigel NJOZ 2015, 41, 42.
[51] Begründung BT-Drs 17/5335, Teil B, zu § 1, S. 13.
[52] Haft/Schlieffen-*Hartmann* § 28 Rn. 17.
[53] Klowait/Gläßer-*Goltermann* § 4 Rn. 35f und Greger/Unberath/Steffek-*Greger* MediationsG § 4 Rn. 10. Einschränkend dagegen Haft/Schlieffen-*Hartmann* § 28 Rn. 19, sowie bspw. Art. 9 der ICC Mediation Rules, die explizit die Verfahrensexistenz von der Vertraulichkeitspflicht ausklammern, siehe https://iccwbo.org/publication/arbitration-rules-and-mediation-rules/.

jedermann enge, gesetzlich normierte Anzeigepflichten für geplante, katalogartig aufgezählte besonders schwerwiegende Straftaten bestehen[54].

Gemäß § 4 S. 4 MediationsG hat der Mediator die Parteien über den Umfang der Verschwiegenheitspflicht in Kenntnis zu setzen. Sie ist dem Auftrag der Mediations-RL entsprechend[55] über das Zeugnisverweigerungsrecht in § 383 Abs. 1 Nr.6 ZPO[56] und den darauf referenzierenden Prozessordnungen[57] abgesichert und überdies gem. § 4 S. 1 MediationsG als Pflicht zur Zeugnisverweigerung ausgestaltet[58]. Diese Regelungen stehen – ebenso wie die Nichtöffentlichkeit – zur Disposition der Parteien, die den Mediator gemäß § 385 Abs.2 ZPO einvernehmlich von seiner Verschwiegenheitspflicht entbinden können. Im Strafprozessrecht findet sich dagegen keine entsprechende Absicherung; erst recht fehlt ein allgemeines Beweisverwertungsverbot in Entsprechung zu Art 20 UNCITRAL Conciliation Rules[59].

Die Verschwiegenheitspflicht des Mediators dient dem ex-ante-Interesse der Parteien, sich auf die Mediation einzulassen und den Weg zu einer einvernehmlichen Einigung zu beschreiten[60]. Zu wissen, dass der Mediator vertrauliche Sachverhalte und Erkenntnisse aus dem Mediationsverfahren seinerseits nicht nach außen tragen darf, und hierzu auch von der anderen Partei beim Scheitern der Mediation im anschließenden streitigen Verfahren nicht als Zeuge benannt werden darf, fördert überdies das Vertrauen in die offene Atmosphäre der Mediation selbst. Die Pflicht wird daher – wie der Ausschluss der Öffentlichkeit – durch das Interesse der Parteien an einem konstruktiven offenen Gespräch über Konflikthintergründe, Motive und Lösungsoptionen im Sinne ihrer Privatautonomie begründet.

3.3. Vertraulichkeitspflichten der Parteien untereinander

Die Interessenlage der Parteien im Hinblick auf die Vertraulichkeit untereinander ähnelt den Interessen in Bezug auf die Verschwiegenheitspflicht des Mediators: Der

---

[54] Klowait/Gläßer-*Goltermann* § 4 Rn. 33.
[55] Siehe EG 23 zur Mediations-RL.
[56] Begr. BT-Drs 17/5335, Teil B zu § 4, S. 17.
[57] Siehe die Auflistung bei Klowait/Gläßer-*Goltermann* § 4 Rn. 9.
[58] So bereits hervorgehoben in BT-Drs 17/5335 Teil B. Lösung, S. 1.
[59] DAV Stellungnahme MediationsG (2010), S. 5f. und auch Wagner ZKM 2010, 172, 174. Näheres zu den UNCITRAL Conciliation Rules in Abschnitt 3.3.
[60] Wagner ZKM 2010, 172, 173f.

jeweils offenbarenden Partei ist der Schutz derjenigen Informationen wichtig, die durch die Durchführung des Mediationsverfahrens der anderen Partei bekannt werden. Beide Medianden sind an einer vertrauensvollen Gesprächsführung interessiert, die in einer offenen Atmosphäre den Austausch über Sichtweisen, Bedürfnisse und damit korrespondierende Lösungsoptionen ermöglicht, um eine **Basis für konstruktive Zusammenarbeit** zu schaffen[61]. Nur unter dieser Prämisse ergibt die Mediation anstelle eines streitigen Verfahrens für beide Seiten Sinn.

Der Austausch über die den Positionen zugrundeliegenden innere Überzeugungen, Gefühle und Konfliktursachen soll insbesondere ohne Belastung durch prozesstaktische Überlegungen erfolgen[62]. Keine Partei, die vertrauliche Informationen äußert oder persönliche Motive für ihr Verhalten offenbart, soll damit rechnen müssen, dass die empfangende Partei ihre Erkenntnisse aus diesen Erklärungen und Verhaltensweisen während der Mediation im Falle ihres Scheiterns anschließend im Gerichtsprozess als Parteivortrag zu Lasten der offenbarenden Partei einbringt[63]. Allerdings finden sich weder in der Mediations-RL noch im MediationsG dazu Regelungen[64]. Die in § 4 Abs. 1 MediationsG geregelte Verschwiegenheitspflicht trifft gemäß der Gesetzesbegründung nur den Mediator und seine Hilfspersonen, insbesondere jedoch nicht die Parteien und deren Hilfspersonen[65].

Demgegenüber sehen Verfahrensordnungen für Mediation[66] und insbesondere Art. 14 der bereits im Jahr 1980 als Vorschlag für vertragliche Vereinbarungen[67] konzipierten und im Vorfeld der Schaffung des Mediationsgesetzes viel zitierten

---

[61] Wagner ZKM 2011, 164, 164.

[62] Greger/Unberath/Steffek-*Greger* MediationsG § 4 Rn. 1

[63] Wagner ZKM 2010, 172, 174 u. Wagner ZKM 2011, 164, 165f. mit Beispielen aus der Praxis.

[64] Siehe auch bereits den rechtspolitischen Vorschlag von Spindler, Gerichtsnahe Mediation, S. 55f und die Kritik von Greger Stellungnahme MediationsG I, S. 5f. und Greger Stellungnahme MediationsG II, S. 9, jeweils explizit im Vergleich zu Art. 10 bzw. Art. 20 UNCITRAL Conciliation Rules, sowie Wagner ZKM 2010, 172, 174 u. die explizite Befürwortung eines Beweisverwertungsverbots bei RTMKM ZKM 2009, 147, 151, sowie bei Löer ZKM 2010, 179, 181 u. DRB Stellungnahme MediationsG (2010), Ziff. 5 S. 4f.

[65] Begr. BT-Drs 17/5335, Teil B zu § 4, S. 17.

[66] Wagner ZKM 2011, 164, 166ff. u. insbes. Art. 9 der ICC Mediation Rules (2014), unter https://iccwbo.org/publication/arbitration-rules-and-mediation-rules/.

[67] Siehe die Erläuterung unter https://uncitral.un.org/en/about/faq/texts.

UNCITRAL Conciliation Rules[68] für Mediationen (bzw. Schlichtungen[69]) in internationalen Wirtschaftskonflikten durchaus die ausdrückliche Pflicht der Parteien vor, alle Angelegenheiten im Zusammenhang mit dem gewählten Konfliktlösungsverfahren geheim zu halten. Sie ist durch ein allgemeines Beweisverwertungsverbot in Art. 20 abgesichert und umfasst insbes. Äußerungen der Gegenseite zu möglichen Beilegungsoptionen ebenso wie Eingeständnisse, Lösungsvorschläge oder die Äußerung der anderen Partei, dass sie einen Lösungsvorschlag für akzeptabel halte.

Noch ausführlicher sind die Regelungen in Artt. 10f. des UNCITRAL Model Law on International Commercial Mediation and International Settlement Agreements Resulting from Mediation, das im Jahre 2018[70] von der UN als Empfehlung an nationale Gesetzgeber für die Mediation internationaler Wirtschaftsstreitigkeiten beschlossen wurde[71]. Auch hiernach sind – abgesehen von geregelten Ausnahmen und vorbehaltlich abweichender Parteivereinbarung – alle Informationen in Bezug auf das Mediationsverfahren vertraulich zu behandeln und unterliegen in nachfolgenden streitigen Verfahren einem Beweisverbot. Hiervon umfasst sind insbes. bereits das Angebot zur Durchführung einer Mediation oder dessen Annahme, Äußerungen oder Vorschläge zu Lösungsoptionen einer Partei, Feststellungen oder Eingeständnisse, Vorschläge des Mediators und befürwortende Stellungnahmen einer Partei dazu, sowie Dokumente, die ausschließlich für die Durchführung der Mediation erstellt wurden. Ausnahmen werden für bereits vorbekannte Tatsachen oder anderweitig zulässige Beweismittel geregelt.

Mangels unmittelbarer Geltung dieser Normen ist eine auf den spezifischen Interessenschutz der Parteien zugeschnittene **Abrede** erforderlich, die sich inhaltlich an den vorgestellten UNCITRAL Regelungen orientieren kann. Es ist allgemein üblich und ratsam, dass die Parteien gleich zu Beginn des Mediationsverfahrens

---

[68] UNCITRAL Conciliation Rules (1980), von der UN Generalversammlung am 4. Dezember 1980 durch Resolution 35/52 beschlossen, abrufbar unter https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/en/conc-rules-e.pdf.

[69] Zur Verwendung des Begriffs „Conciliation" für Mediation, siehe die Fußnote 1 auf S. 1 des UNCITRAL Model Law on International Commercial Mediation and International Settlement Agreements Resulting from Mediation.

[70] UNCITRAL Model Law on International Commercial Mediation and International Settlement Agreements Resulting from Mediation (2018), von der Generalversammlung am 20. Dezember 2018 durch Resolution 73/199 angenommen, abrufbar unter https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/en/annex_ii.pdf.

[71] Siehe die Erläuterung unter https://uncitral.un.org/en/about/faq/texts.

Vereinbarungen zur gebotenen Vertraulichkeit treffen, die auch zugleich die Nichtverwertung dieses Materials in ggf. nachfolgenden streitigen Verfahren regeln[72].

Diese frühzeitige Betonung der Möglichkeit des Scheiterns der Mediation und seiner Folgen kann die konstruktive Einstellung der Parteien beeinträchtigen, zur Zurückhaltung der Parteien während der Mediation führen und die Schaffung der erforderlichen Vertrauensbasis behindern[73]. Dadurch, dass der Gesetzgeber diese Verantwortung den Parteien überträgt, wird jedoch deren Autonomie und Gestaltungsfreiheit betont. Die vorweggeschaltete Klärung und einvernehmliche Vereinbarung auf Veranlassung des Mediators sind für die erfolgreiche Durchführung der Mediation erforderlich und schaffen erste Erfahrungen mit Mediationspraktiken – in Bezug auf das Verfahren, nicht auf den Konfliktgegenstand[74].

Derartige Vereinbarungen, durch die sich die Parteien verpflichten, bestimmte Tatsachen nicht vorzutragen bzw. bestimmte Beweismittel nicht zu benennen, sind aufgrund des im Zivilprozessrechts geltenden Dispositionsgrundsatzes und der Verhandlungsmaxime auch wirksam und berechtigen die Gegenseite zur Einrede[75]. Prozessverträge bewirken jedoch kein Beweisverwertungsverbot[76] und gelten auch nicht im Bereich des Strafprozessrechts.

Auf die Umsetzung der Vertraulichkeitspflichten bei der Durchführung der Mediation mittels Videokonferenz wird in Abschnitt 6 eingegangen.

---

[72] Haft/Schlieffen-*Hartmann* § 28 Rn. 33; Haft/Schlieffen-*Kracht* § 13 Rn. 121.

[73] Wagner ZKM 2011,164, 164f.

[74] Haft/Schlieffen-*Kessen/Troja* § 14 Rn. 19.

[75] BGH Urt. v. 21.12.1960 – VIII ZR 204/59, veröff. in BGHZ 34, 254, 258; Haft/Schlieffen-*Hartmann* § 28 Rn. 39ff. m. w. N.

[76] Haft/Schlieffen-*Hartmann* § 28 Rn. 40f.

4. Datenschutzrecht

Zusätzlich zu den aus dem Vertraulichkeitsgrundsatz folgenden Pflichten der am Mediationsverfahren Beteiligten ergeben sich auch aus dem Regelungsbereich des Datenschutzrechts besondere Aufgaben und Verantwortlichkeiten. Das Nebeneinander der gesetzlichen Vorschriften des Datenschutzrechts und der mediationsspezifischen Vertraulichkeits- und Verschwiegenheitsregelungen führt in der Praxis zu Überschneidungen. Die Rechtsquellen werden im Folgenden überblicksartig dargestellt, bevor auf die damit verbundene Interessenlage eingegangen wird.

4.1. Begriff „Datenschutz“ und historischer Rückblick

Zum Verständnis der rechtlichen Grundlagen und der Interessenbetrachtung ist es notwendig, auf die Ursprünge des Datenschutzrechts einzugehen.

Der Begriff „Datenschutz“ ist missverständlich, denn eigentlich geht es beim Datenschutz nicht im Kern um den Schutz der Daten selbst, sondern um den Schutz des Betroffenen vor den Konsequenzen der Verarbeitung seiner personenbezogenen Daten[77]. Die Terminologie hat sich jedoch zunächst in Deutschland und dann auf europäischer Ebene[78] sowie stellenweise global[79] etabliert. Parallel dazu findet man im englischsprachigen Raum auch den unschärferen Begriff „privacy“[80], der zwar in seinen Ursprüngen den Schutz der Privatsphäre und der Unverletzlichkeit der Wohnung im Blick hatte[81], inzwischen jedoch – zumindest im anglo-amerikanischen Kontext – oft auch anstelle des Begriffs „Datenschutz“ verwendet wird. Dies hat sich teilweise in die datenschutzrechtliche Terminologie im europäischen

[77] Simitis/Hornung/Spiecker-*Simitis/Hornung/Spiecker gen. Döhmann* Einl. Rn. 2.
[78] Siehe die einzelnen Sprachfassungen der DSGVO unter https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=celex%3A32016R0679.
[79] Siehe bspw. für die Aufsichtsbehörden in Singapur unter https://www.pdpc.gov.sg/.
[80] Siehe den Hinweis des EDSB unter https://edps.europa.eu/data-protection/data-protection_de.
[81] Siehe dazu bereits im Jahre 1948 als Abwehrrechte in Art. 12 AEMR und Art. 8 EMRK mit positiver Formulierung und Gesetzesvorbehalt.

Sprachraum übertragen, obgleich im Zusammenhang der EU-Regelungen[82] dagegen weiterhin zwischen „Privacy" als dem Schutz der Privatsphäre im Allgemeinen und „Datenschutz" als dem spezielleren Schutz der personenbezogenen Daten einer Person unterschieden wird[83].

Entwicklungen in Deutschland: Nachdem das Bundesland Hessen bereits im Jahre 1970 insbesondere als Reaktion auf zunehmend automatisierte Datenverarbeitung in der öffentlichen Verwaltung[84] das weltweit erste Datenschutzgesetz erließ[85], folgte zum 01.01.1978 das Bundesdatenschutzgesetz (BDSG)[86]. Die Überarbeitung in den Folgejahren führte zu bedeutenden Novellen insbesondere in den Jahren 1990[87] anlässlich des sog. „Volkszählungsurteils" des Bundesverfassungsgerichts[88], sowie 2001[89] aufgrund der europäischen Datenschutz-RL und 2018[90] sowie 2019[91] aufgrund der DSGVO (zu beidem sogleich).

Entwicklungen in Europa: Auf europäischer Ebene trat zunächst die europäische Datenschutz-RL im Jahre 1995 in Kraft. Sie wurde – in Umsetzung des Art. 8 GRCh geregelten expliziten Grundrechts auf Schutz personenbezogener Daten – durch die Datenschutzgrundverordnung der Europäischen Union (DSGVO) am 25. Mai 2018 abgelöst, siehe Art 94 Abs. 1 DSGVO[92].

---

[82] Siehe dazu insbesondere bereits die Unterscheidung in Art. 7 und Art. 8 GRCh, sowie die zahlreichen Regelungen der ePrivacy-RL, in denen beide Begriffe parallel und mit unterschiedlichem Anwendungsbereich verwendet werden.

[83] Siehe auch die Erläuterung auf den Seiten des EDSB unter https://edps.europa.eu/data-protection/data-protection_en. und zum dogmatischen Unterschied s. u. in Abschnitt 4.2.

[84] Simitis/Hornung/Spiecker-*Simitis/Hornung/Spiecker gen. Döhmann* Einl. Rn. 6ff.

[85] Zu den Hintergründen und zu seinem Urheber und Wegbereiter des Datenschutzes siehe insbesondere das Interview von Bernd Frye mit Spiros Simitis: Frye/Simitis, Forschung Frankfurt 2015, 44ff.

[86] BGBl. 1977 Teil I, S. 201.

[87] BGBl. 1990 Teil I, S. 2954.

[88] BVerfG, Urt. v. 15.12.1983 – 1 BvR 209/83 – BVerfGE 65, 1ff.

[89] BGBl. 2001 Teil I, S. 904.

[90] BGBl. 2017 Teil I, S. 2097.

[91] BGBl. 2019 Teil I, S. 1626, dort 1633.

[92] In Art. 288 AEUV sind die verschiedenen Rechtsakte geregelt, die von den EU-Organen erlassen werden können, insbesondere die Verordnung (Abs. 2) und die Richtlinie (Abs. 3). Verordnungen gelten in allen EU-Mitgliedstaaten unmittelbar als nationales Recht für alle Adressaten. Richtlinien verpflichten dagegen nur die EU Mitgliedsstaaten selbst und müssen von ihnen im nationalen Recht umgesetzt werden (zweistufiger Rechtssetzungsprozess).

Durch die DSGVO wurden die rechtlichen Grundlagen des Datenschutzrechts in den Mitgliedsstaaten mit dem Ziel der Anpassung an moderne technologische Entwicklungen harmonisiert[93], auch wenn eine Reihe von Öffnungsklauseln abweichende, insbesondere striktere Regelungen nationaler Gesetzgeber zulassen[94]. Gegenüber der in ihrem Geltungsbereich unmittelbar anzuwendenden DSGVO gilt das BDSG gemäß § 1 Abs. 5 BDSG nachrangig, daher geht die vorliegende Arbeit systematisch auf die grundlegenden Pflichten der DSGVO ein und stellt nur – wo erforderlich – Abweichungen oder Ergänzungen des BDSG und anderer einschlägiger Gesetze dar.

4.2. Interessenlage

Nach europäischer Rechtsauffassung ist das in Art. 8 GRCh explizit geregelte Recht auf Datenschutz eine besondere Ausprägung des Privatsphäre-Schutzes in Art. 7 GRCh, der sich auf den absoluten Schutz der Menschenwürde zurückführen lässt[95], bzw. eine besondere Form des Achtung des Privat- und Familienlebens im Sinne von Art. 8 EMRK[96]. Die Schutzgutanalyse in der DSGVO ist zumindest ihrem Wortlaut nach allerdings nicht eindeutig[97]. Nach der überwiegenden Meinung deutscher Juristen handelt es sich bei dem aus Art. 1 Abs. 1 und Art. 2 Abs. 1 GG folgenden Recht auf „**informationelle Selbstbestimmung**“ um einen Unterfall des ebenfalls aus der Menschenwürde abgeleiteten Allgemeinen Persönlichkeitsrechts[98].

Es geht nicht um einen besonderen Privatsphäreschutz, der im GG vorrangig durch den Schutz des Fernmeldegeheimnisses in Art. 10 GG oder den Schutz der Unverletzlichkeit der Wohnung gemäß Art. 13 GG gewährleistet wird[99], und nicht

---

[93] Schuster/Grützmacher-*Freund* Vorbem. DSGVO Rn. 1.

[94] Siehe hierzu die Kritik von Schuster/Grützmacher-*Freund* Vorbem. DSGVO Rn. 4.

[95] So unter https://edps.europa.eu/data-protection/data-protection_de.

[96] So EG 2 zur Datenschutz-RL und auch der EuGH in weiteren zeitlich nachfolgenden Entscheidungen, siehe Michl, DuD 2017, 349, 350ff.

[97] Siehe die schon fast satirische Beschreibung der Vielfalt der in der DSGVO erwähnten Schutzgüter bei Veil, CR-online.de Blog, 22.04.2021.

[98] So bereits BVerfGE 65, 1, 42 (Rn. 143).

[99] Das liegt nahe, wenn man undifferenziert den Begriff „Privacy“ als Privatsphäre-Schutz auch für Datenschutzfragen verwendet, siehe bereits oben Abschnitt 4.1.

um „Eigentum an den Daten“[100], sondern um den letztlich direkt in der Unantastbarkeit der Menschenwürde verwurzelten Schutz des Bedürfnisses des Einzelnen nach Autonomie , Freiheit und Sicherheit[101].

Das ureigene Interesse jedes Menschen, grundsätzlich selbst über das Ob und das Wie einer Offenlegung oder Verwendung seiner persönlichen Daten entscheiden zu dürfen[102], d. h. der Wunsch jedes Einzelnen autonom zu bestimmen, welche Informationen, die ihn direkt selbst betreffen, wann, in welchem Umfang und zu welchem Zweck, durch wen und wie lange erhoben und verarbeitet werden, entstammt dem individuellen Interesse sich nach den eigenen Vorstellungen zu entwickeln[103]. Diese Überlegungen liegen dem das Datenschutzrecht prägenden Einwilligungsvorbehalt zugrunde: Eine Verarbeitung ist gem. Art. 6 Abs. 1 lit. a) DSGVO grundsätzlich nur dann und nur in dem Umfang zulässig, in dem der Betroffene freiwillig sein Einverständnis hierzu gegeben hat.

Dieses freiheitsschützende Grundrecht wird den Individuen jedoch im Sinne eines funktionierenden Gemeinwesens nicht absolut und schrankenlos gewährt. Jeder Mensch ist als Mitglied der sozialen Gemeinschaft im Rahmen seiner Persönlichkeitsentwicklung auch auf Kommunikation und damit Informationspreisgabe angewiesen[104]. In Fällen, in denen ein Interesse der Allgemeinheit an der Verarbeitung konkreter Daten überwiegt, muss im Sinne der „Gemeinschaftsbezogenheit und Gemeinschaftsgebundenheit der Person“[105] das Recht auf informationelle Selbstbestimmung begrenzt werden können[106].

Im Sinne des Sicherheitsbedürfnisses des Einzelnen ist gem. dem Rechtsmäßigkeitsprinzip des Art. 6 Abs. 1 DSGVO eine Verarbeitung personenbezogener Daten als Eingriff nur auf der Grundlage und im Rahmen geltenden Rechts[107], d. h. mangels Einwilligung des Betroffenen nur gemäß einem anderen Erlaubnistatbestand

---

[100] So frühere Rechtsauffassungen aus den Siebzigerjahren, d. h. vor Schaffung des ersten Datenschutzgesetzes, siehe Simitis/Hornung/Spiecker-*Simitis/Hornung/Spiecker gen. Döhmann* Einl. Rn. 27 m. w. N.

[101] Im Einzelnen sind die dogmatischen Beziehungen zwischen Artt. 7 u. 8 GRCh, sowie zwischen dem Recht auf informationelle Selbstbestimmung und dem Fernmeldegeheimnis in Art. 10 GG durchaus umstritten, siehe dazu im Einzelnen Michl, DuD 2017, 349ff und Papier Vortrag 2010.

[102] BVerfGE 65, 1, 42 (Rn. 144).

[103] Simitis/Hornung/Spiecker-*Simitis/Hornung/Spiecker gen. Döhmann* Einl. Rn. 32.

[104] BVerfGE 65, 1, 44 (Rn. 148).

[105] BVerfGE 65, 1, 44 (Rn. 148).

[106] Simitis/Hornung/Spiecker-*Simitis/Hornung/Spiecker gen. Döhmann* Einl. Rn. 34.

[107] Simitis/Hornung/Spiecker-*Simitis/Hornung/Spiecker gen. Döhmann* Einl. Rn. 33.

des Art. 6 DSGVO zulässig. Hierdurch wird, ebenso wie durch Art. 8 Abs. 2 GRCh, das Interesse des Einzelnen an Rechtssicherheit und insbesondere auch am Schutz vor staatlicher Willkür betont: Soweit gesetzliche Regelungen den Eingriffen zugrunde liegen, müssen diese den Geboten von **Klarheit und Verhältnismäßigkeit** genügen[108] und zudem den Verwendungszweck der Daten beschreiben[109]. Das Recht auf Datenschutz muss dabei abgewogen werden gegen andere Werte der Gesellschaft, gegen Menschenrechte Dritter oder öffentliche Interessen, wie z. B. die nationale Sicherheit[110], sowie das Funktionieren des europäischen Binnenmarktes, zu dem auch der freie Informationsfluss gehört[111]. Die DSGVO dient dabei neben der Regulierung internationaler Datenströme (insbesondere durch die Verbreitung des Internet)[112] explizit auch der Schaffung der für das Wachstum der digitalen Wirtschaft im EU-Binnenmarkt erforderlichen Vertrauensbasis und Rechtssicherheit[113]. Die gesetzliche Interessenabwägung muss das jeweilige Allgemeininteresse genau bezeichnen und zu den möglichen Folgen der Verarbeitung für den Betroffenen ins Verhältnis setzen[114] oder dies dem Eingreifenden vorschreiben.

Ursprünglich stand die „Furcht vor einer unkontrollierten Persönlichkeitserfassung" insbesondere durch öffentliche Stellen im Fokus der rechtlichen Betrachtung, so z. B. bei der Auseinandersetzung des Bundesverfassungsgerichts mit dem VZG 1983[115]. Ein Bürger, der besorgt sein muss, dass Informationen in Bezug auf seine Person unkontrolliert und unbegrenzt mit anderen Datensammlungen zu einem Persönlichkeitsbild zusammengefügt werden können[116], wird in der freien Entfaltung seiner Persönlichkeit gehemmt („**Chilling-Effect**"). Dies beeinträchtigt nicht nur – wie dargestellt – die individuelle Autonomie und Freiheit, sondern im größeren Rahmen auch das durch die Handlungs- und Mitwirkungsfähigkeit der Bürger begründete freiheitlich demokratische Gemeinwesen[117]. Zwar war das BDSG in seiner

---

[108] So auch schon BVerfGE 65, 1, 45 (Rn. 149).
[109] BVerfGE 65, 1, 46 (Rn. 151).
[110] So der EDSB unter https://edps.europa.eu/data-protection/data-protection_de und EG 4 zur DSGVO.
[111] Ehmann/Selmayr-*Zerdick* Art. 1 Rn. 2.
[112] Simitis/Hornung/Spiecker-*Simitis/Hornung/Spiecker gen. Döhmann* Einl. Rn. 208.
[113] EG 7 zur DSGVO.
[114] Simitis/Hornung/Spiecker-*Simitis/Hornung/Spiecker gen. Döhmann* Einl. Rn. 43.
[115] BVerfGE 65, 1, 41ff. (Rn. 143ff.)
[116] BVerfGE 65, 1, 42 (Rn. 145).
[117] BVerfGE 65, 1, 43 (Rn. 146), jedoch nicht ausdrücklich in den Erwägungsgründen der DSGVO, siehe Simitis/Hornung/Spiecker-*Simitis/Hornung/Spiecker gen. Döhmann* Einl. Rn. 235.

ersten Fassung 1978 bereits in seinem § 2 Abs. 2 sowohl auf den Schutz der personenbezogenen Daten gegen Eingriffe durch staatliche Stellen wie auch durch private Stellen ausgerichtet. Insbesondere in den Folgejahren richtete sich die Hauptsorge vor unüberschaubarer und unbegrenzter Datenverarbeitung jedoch vorrangig gegen das Handeln der öffentlichen Verwaltung[118].

Inzwischen überwiegt aufgrund der Entwicklung des Internet und der mit seiner Nutzung einhergehenden „**Big-Data Gefährdungslage**“[119] die Sorge vor Datensammlungen privater Anbieter[120], wie beispielsweise Facebook oder Google. Insbesondere bei der Diskussion über den Schutz vor Eingriffen privater Stellen im Kontext der Internetnutzung wird inzwischen sogar die offene Frage gestellt, ob das Recht auf informationelle Selbstbestimmung überhaupt noch gewünscht sei: Die Verfechter einer „Post Privacy World“ verweisen darauf, dass Mitglieder sozialer Netzwerke ohnehin in aller Öffentlichkeit und absichtlich Informationen verbreiteten, die nach überkommener Überzeugung der Privatsphäre zuzuordnen seien (so z. B. Informationen über den aktuellen eigenen Gesundheitszustand)[121]. Die Grenzen zwischen Öffentlichkeit und Privatheit seien im Begriff zusehends zu verschwimmen[122]. Der pauschalen Behauptung „Privacy is dead“ folgt dann aber noch im gleichen Atemzug geradezu widersprüchlich die Forderung nach einer „regulierten Transparenz“[123]. Aus rechtlicher Sicht ist das Grundrecht auf informationelle Selbstbestimmung daher keineswegs obsolet.

4.3. Zentraler Anknüpfungspunkt

Die datenschutzrechtlichen Pflichten sind in der DSGVO deutlich detaillierter beschrieben als die aus dem Kontext der Vertraulichkeit entstehenden drei Grundpflichten im MediationsG. Daher werden sie zweckmäßigerweise zusammen mit der Beschreibung der konkreten Umsetzung in der Praxis in Abschnitt 7 dargestellt.

---

[118] So auch spezifisch einschränkend BVerfGE 65, 1, 45f. (Rn. 150)
[119] So Michl DuD 2017, 349, 352.
[120] Hornung MMR 2004, 3, 6 und Papier Vortrag 2010, S. 6f., aber auch EG 6 zur DSGVO.
[121] Schertz Vortrag 2013, S. 2f.
[122] Schertz Vortrag 2013, S. 7.
[123] So bereits Spivak Wired 2013.

Der vorliegende Abschnitt beschränkt sich demnach auf die Erläuterung des Grundbegriffs der Verarbeitung personenbezogener Daten in der Leitnorm des Art. 1 Abs. 1 DSGVO, anhand der die grundsätzliche Relevanz des Datenschutzrechts für die Mediatorentätigkeit gezeigt wird.

Personenbezogene Daten sind gem. Art. 4 Nr. 1 DSGVO weit definiert und bezeichnen alle Informationen, die einer „betroffenen Person" zugeordnet werden können, sei es direkt, oder indirekt unter Zuhilfenahme weiterer Informationen[124]. Betroffene Personen sind dabei – anders als beispielsweise im schweizerischen Datenschutzrecht (Art. 3 lit. b DSG-CH) – nur natürliche, nicht juristische Personen[125].

Dies umfasst im Kontext der Mediation insbesondere Informationen wie Name, Telefonnummer, Emailadresse und Anschrift sowie bspw. Bankverbindung der Parteien selbst[126] bzw. ihrer Vertreter, wenn die Parteien juristische Personen sind. Neben überprüfbaren oder auch wahren Tatsachen sind auch im Rahmen des Mediationsgesprächs geäußerte Behauptungen und Meinungen, Vermutungen und Werturteile über Personen von diesem Begriff umfasst. Und schließlich sind ggf. Informationen mit Bezug zu weiteren Konfliktbeteiligten oder aus Schilderungen über den Konflikthintergrund einzubeziehen.

Die Beschreibung der Vorgänge, auf die die DSGVO anwendbar ist, ist als **Verarbeitung** gem. Art. 4 Nr. 2 DSGVO denkbar weit definiert. Ausgehend von der durch die DSGVO ersetzten Datenschutz-RL und in Abweichung zu vorhergehenden nationalen Gesetzen wie bspw. dem BDSG a. F.[127], fehlt eine Strukturierung in feste tätigkeitsbeschreibende Fallgruppen. Stattdessen wird der Begriff allgemein umschrieben und dann anhand von nicht abschließend aufgezählten Beispielen erläutert[128]. Er umfasst sämtliche denkbaren Tätigkeiten, die einen Umgang mit personenbezogenen Daten darstellen[129], von der Erhebung, über das Speichern, Ordnen und Ändern, bis hin zum Offenlegen oder Löschen.

---

[124] Simitis/Hornung/Spiecker-*Karg* Art. 4 Nr. 1 Rn. 43 und Rn. 46.

[125] Simitis/Hornung/Spiecker-*Karg* Art. 4 Nr. 1 Rn. 38. Ehmann/Selmayr-*Klabunde* Art. 4 Nr. 1 Rn. 12 u. Rn. 14.

[126] Siehe auch Bertolino ZKM 2019, 58, 58.

[127] D. h. in der Fassung vor der Novelle im Jahre 2018.

[128] Simitis/Hornung/Spiecker-*Roßnagel* Art. 4 Nr. 2 Rn. 2ff., insbes. Rn. 4.

[129] Simitis/Hornung/Spiecker-*Roßnagel* Art. 4 Nr. 2 Rn. 4 und Rn. 11.

Grundsätzlich irrelevant ist es für den Verarbeitungsbegriff in Art. 4 Nr. 2 DSGVO, ob der Vorgang manuell oder automatisiert erfolgt[130]. Es unterliegen jedoch nicht alle Handlungen im Mediationsbüro, die personenbezogene Daten tangieren, auch datenschutzrechtlichen Pflichten[131], denn in Art. 2 Abs.1 i. V. m. Art. 4 Nr. 6 DSGVO wird der sachliche Anwendungsbereich der DSGVO beschränkt: Manuelle Verarbeitungen werden den (zumindest teilweise) mithilfe von Informationstechnik durchgeführten Vorgängen nur dann gleichgestellt, wenn durch sie eine Verarbeitung personenbezogener Daten in strukturierten Dateisystemen vorliegt, die nach gewählten Kriterien durchsucht werden können[132]. Blattsammlungen, manuelle Falldokumentation, selbst manuell geführte Akten, und erst recht Flipcharts, auf denen der Mediator den Fortgang der Gespräche visualisiert, sind daher vom Anwendungsbereich der DSGVO nicht umfasst[133]. Hintergrund dieser klaren Trennung manueller und IT-gestützter Verarbeitungstechniken ist die bereits beschriebene Schutzrichtung der DSGVO, die Betroffenen vor der für sie undurchschaubaren und unvorhergesehenen Analyse und Aufbereitung personenbezogener Daten – insbesondere in elektronischer Speicherform – zu bewahren.

Die Verarbeitung muss gemäß Art. 5 Abs. 1 lit. a DSGVO insbesondere rechtmäßig und für den Betroffenen nachvollziehbar sein. Diese Grundsätze bilden die Basis der dann nachfolgenden materiell-rechtlichen Detailregelungen und dienen als deren Auslegungsrichtlinien[134]. Bei der Verarbeitung müssen neben der Anforderung ihrer Rechtmäßigkeit die in Art. 5 Abs. 1 geregelten datenschutzrechtlichen Grundsätze, so bspw. die Zweckbindung in lit. b, die Datenminimierung in lit. c, die Richtigkeit in lit. d, die Speicherbegrenzung in lit. e und die Vertraulichkeit in lit. f beachtet werden. Gem. Artt. 24 Abs. 1, 25 Abs. 1 u. 2, sowie 32 Abs. 1 u. 2 DSGVO hat der Mediator als Verantwortlicher i. S. d. Art. 4 Nr. 7 DSGVO zur Sicherheit der Verarbeitung sowie zur Einhaltung dieser Grundsätze geeignete technische und organisatorische Maßnahmen zu ergreifen.

Zu diesen Details wird – nach der Vorstellung der besonderen vertraglichen Konstellation – im Kontext der Auswahl des geeigneten Videokonferenzdienstes und der Durchführung der Videokonferenz in Abschnitt 7 Stellung zu nehmen sein.

---

[130] Siehe auch den Grundsatz der Technologieneutralität in EG 15 zur DSGVO.

[131] Anders jedoch Bertolino ZKM 2019, 58, 58, Weigel Inkovema Blog 17.02.2020 und Dendorfer-Ditges/Schmidt-Gorbach KD 2018, 318, 318.

[132] Simitis/Hornung/Spiecker-*Roßnagel* Art. 4 Nr. 6 Rn. 7f. und Rn. 14.

[133] Ehmann/Selmayr-*Klabunde* Art. 4 Rn. 35.

[134] Simitis/Hornung/Spiecker-*Roßnagel* Art. 5 Rn. 15.

5. Vertragslage und grundsätzliche Auswahlentscheidung

Zur Klärung, welche Verantwortung den Mediator beim Einsatz von Videokonferenzdiensten treffen, ist zunächst ein Blick auf die verschiedenen Kommunikationsebenen und die dazu erforderlichen Verträge notwendig.

5.1. Telefon-/Internetanschluss

Im ersten Schritt benötigen alle Beteiligten, sowohl der Mediator als auch die Parteien, jeweils einen eigenen technischen Anschluss an das Internet als öffentliches Kommunikationsnetz, und einen darauf bezogenen Vertrag über Internet-Access. Dadurch dass diese Anschlussverträge auf die Nutzung von öffentlich zugänglichen Kommunikationsdiensten ausgerichtet sind und mit Dienstanbietern bestehen, die ihre Leistungen auf Dauer und für eine Vielzahl von Nutzungsfällen anbieten[135], gilt für diese Leistungen das Fernmeldegeheimnis gemäß §§ 88, 107 TKG.

Es schreibt die vertrauliche Behandlung sowohl der Inhalte der Telekommunikation als auch der Telekommunikationsverbindung vor. Hiervon sind neben den Inhaltsdaten (Sprache, Bilder, Text) auch alle Verkehrsdaten zur Identität der Teilnehmenden[136] und zum Zeitpunkt sowie zur Dauer der Verbindung (übergreifend auch „Metadaten" genannt[137]) umfasst. Dadurch werden bei der Nutzung dieser Telekommunikationsdienste – trotz des Einsatzes eines öffentlichen Telekommunikationsnetzwerks – die Vertraulichkeit der Mediation und der Grundsatz der Nichtöffentlichkeit gewahrt. Eine zusätzliche vertragliche Verpflichtung des Anbieters zur Geheimhaltung ist nicht notwendig.

Außerdem gilt für diese Vertragsbeziehungen das telekommunikationsspezifische Datenschutzrecht der §§ 91ff. TKG, das jedoch keine datenschutzrechtliche Auftragsverarbeitungsvereinbarung fordert.

Dadurch, dass alle Parteien gleichermaßen über ihre eigenen Verträge zur Nutzung dieser Infrastruktur verfügen, kommt dem Mediator insoweit keine gesonderte rechtliche Rolle zu. Auf eine tiefergehende Betrachtung wird im Kontext der vorliegenden Arbeit daher verzichtet.

---

[135] Beck TKG-*Bock* § 88 Rn. 22f.
[136] Beck TKG-*Bock* § 88 Rn. 14.
[137] Auer-Reinsdorff/Conrad-*Assion* § 31 Rn. 26.

5.2. Videokonferenzdienste

Über die bestehenden Internet-Anschlussverträge hinaus benötigen der Mediator und die Medianden Verträge zur Teilnahme an der Videokonferenz.

5.2.1. Vertrag zwischen Organisator und Anbieter

Die vertragliche Struktur sieht dabei so aus, dass der Mediator einen kostenlosen oder entgeltlichen Nutzungsvertrag mit dem Anbieter schließt, der ihn zum Organisieren von Konferenzen berechtigt. Dieses als Dienstvertrag zu qualifizierende Dauerschuldverhältnis setzt i. d. R. die Registrierung als Nutzer voraus und ist dann inhaltlich darauf ausgerichtet, dass der Konferenzanbieter dem organisierenden Nutzer ermöglicht, eine Videokonferenz zu einem bestimmten Zeitpunkt zu planen, die Teilnehmer einzuladen, und dann diese Videokonferenz durchzuführen.

Die Leistungen können die Lizenz zum Download und zur Nutzung einer spezifischen Anwendung enthalten. Überdies sind mitunter Supportleistungen, d. h. die Zusage von Funktions- oder Sicherheits-Updates für die eingesetzte Technologie, sowie ggf. ein Kontakt für technische Störungen vereinbart. Weitere optionale Leistungen können Speicherplatz für Konferenzaufzeichnungen oder geteilte Inhalte umfassen. Für jeden einzelnen Nutzungsvorgang ruft der Mediator dann entweder in der Anwendung oder im Webbrowser die Videokonferenz-Funktionalität auf.

Anbieter, wie z. B. die Horizon44 GmbH mit dem Dienst „sichere-videokonferenz.de“[138], ermöglichen jedem Besucher der Webseite ohne Nutzerkonto-Registrierung und damit ohne übergreifenden Vertrag schlicht die punktuelle Einrichtung und Nutzung einer Videokonferenz. Dazu wird auf Anfrage bei jedem Webseiten-Besuch ein individueller Link für die einzurichtende Konferenz erstellt, der vom Organisator mit den anderen Teilnehmern geteilt werden kann. Damit beschränkt sich die vertragliche Beziehung des Mediators als Konferenzveranstalter zum Dienstanbieter jeweils auf den einzelnen Nutzungsvorgang.

5.2.2. Vertrag zwischen Teilnehmer und Anbieter

Jeder Teilnehmer wiederum, also vorliegend die Medianden, erhält vom Mediator über Email einen Link oder Einwahldaten, so dass er ebenfalls mittels Webbrowser oder mit einer speziellen heruntergeladenen App an der Videokonferenz teilnehmen

[138] Siehe unter https://sichere-videokonferenz.de/.

kann. Unabhängig davon, ob die Teilnahme ein Benutzerkonto erfordert und davon, ob sie über eine speziell herunterzuladende Anwendung oder schlicht über den beim Nutzer vorhandenen Webbrowser auf dem Endgerät erfolgt, schließen auch die Parteien eigene Verträge mit dem Dienstanbieter, deren Inhalt dann zumindest die Ermöglichung der Teilnahme an der Videokonferenz umfasst.

Es entsteht also ein Dreiecksverhältnis: Neben dem Vertrag zwischen dem Mediator und dem Dienstanbieter und dem Mediationsvertrag zwischen dem Mediator und den Parteien, der die Nutzung der Videokonferenz zu Mediationszwecken regelt, bestehen jeweils zwischen jeder Partei und dem Dienstanbieter zur Verträge zur Nutzung der Infrastruktur im Rahmen der organisierten Videokonferenz.

5.3. Auswahlentscheidung

Wie bei der Entscheidung für eine bestimmte Lokation für die Mediationsdurchführung vor Ort[139] stellt sich auch beim Einsatz eines Videokonferenztools die Frage der Geeignetheit.

Es gibt mittlerweile eine Fülle von kostenlosen Angeboten, die mit unterschiedlichen Schwerpunkten (insbesondere Sicherheit, Datenschutz und Nutzerfreundlichkeit) oder auch Funktionsreichhaltigkeit beworben werden. Daneben ist zwischen kostenlosen Diensten und solchen zu unterscheiden, die gegen Entgelt wiederum erhöhte Sicherheit, erweiterte Nutzungsrechte (Dauer, Teilnehmer, Nutzerkonten) oder Zusatzfunktionen (Aufzeichnung, Speicherplatz) bieten. Es gibt dabei Merkmale, die allen gemeinsam sind (bspw. Audio- und Videoübertragung, Transportverschlüsselung), aber auch Unterschiede, die dann vom Mediator eine jeweils angepasste Handhabung erfordern. Teilnehmer können sich z. T. schlicht über ihren Webbrowser einwählen, z. T. ist ein Nutzerkonto auch für sie erforderlich, oder sogar der Download einer Anwendung.

Ein kompletter Vergleich der in Frage kommenden Videokonferenzdienste würde den Rahmen dieser Arbeit sprengen. Übersichten sind im Internet an verschiedenen Stellen veröffentlicht[140], und eine Evaluation einiger gängiger Dienste in funktionaler Hinsicht ist zumindest für mediationsnahe Verfahren verfügbar[141].

---

[139] Dazu Troja ZKM 2009, 152, 154.

[140] Siehe bspw. https://www.werockyourweb.com/office/communication/video-conferencing/; (Stand: 20.07.2020); https://de.wikipedia.org/wiki/Liste_von_Webkonferenz-Software (Stand: 16.10.2020); und https://www.computerwoche.de/a/die-wichtigsten-videokonferenz-systeme,3548602 (Stand: 29.10.2020), sowie GDD Praxishilfe DS-GVO XVI Anlage II (Stand: Januar 2021).

[141] Kilburg Komet Blog 14.07.2020 oder auch BRAK Übersicht VK (Stand: Januar 2021).

Jede Gegenüberstellung ist zudem nur eine Momentaufnahme, da sich die Dienste im Hinblick auf Funktionen, Sicherheit, Verfügbarkeit und Vergütungsstrukturen fortlaufend weiterentwickeln. In **Anhang 1** ist daher eine grundlegende Checkliste beigefügt, die u. a. eine strukturierte Prüfung der Funktionsmerkmale, aber insbesondere auch der Sicherheits- und Datenschutzanforderungen unterstützt. Auf das Erforderlichkeitskriterium für die Funktionalitäten des Dienstes ist im Kontext Datenschutz näher einzugehen (s. u. Abschnitt 7.4.1).

Wählt der Mediator den Konferenzdienst (ggf. zusammen mit den Parteien) aus, ist es empfehlenswert, dass er nach seiner eigenen Information mithilfe der Checkliste anschließend die im Kontext der Vertraulichkeit und des Datenschutzes spezifischen Besonderheiten mit den Parteien erörtert[142], den passenden Dienst und geeignete Regeln vereinbart. Haben die Parteien dagegen selbst Erfahrungen mit dem Durchführen einer Videokonferenz und eine Präferenz für einen bestimmten Anbieter oder Dienst, kann die Erläuterung durch den Mediator und die entsprechende Vereinbarung unter Hinweis auf den Parteiwunsch kürzer ausfallen.

Im Folgenden soll nun auf die besonderen Fragestellungen der Vertraulichkeit und des Datenschutzes bei der Durchführung der Mediation über Videokonferenz eingegangen werden. Dabei wird beispielhaft auf Dienstanbieter eingegangen, die im Kontext des Datenschutzes in Abschnitt 7 näher vorgestellt werden.

---

[142] Gläßer/Sinemillioglu/Wendenburg ZKM 2020, 80, 83.

6. Vertraulichkeitsfragen bei Mediation über Videokonferenz

Im Kontext des mediationsrechtlichen Vertraulichkeitsgrundsatzes werden dessen drei Elemente nacheinander im Hinblick auf Besonderheiten und Pflichten der Beteiligten speziell bei der videokonferenzgestützten Mediation untersucht. Eine Liste mit praktischen Hinweisen in **Anhang 2** fasst die wichtigsten Punkte zusammen.

6.1. Nichtöffentlichkeit

Zunächst ist der Grundsatz der Nichtöffentlichkeit zu betrachten. Ebenso wie bei Mediationen vor Ort dürfen nur die Medianden und einvernehmlich von ihnen gemäß § 2 Abs. 4 MediationsG bestimmte Dritte (z. B. ihre Rechtsanwälte oder Steuerberater) an der Mediation teilnehmen. Hier stellen sich bei der Durchführung der Mediation im Wege der Videokonferenz besondere Herausforderungen:

6.1.1. Einladung

So, wie vor Ort nur die Teilnehmer eingeladen werden, darf auch die Einladung für die Videokonferenz nur den Personen zugehen, die teilnahmeberechtigt sind. Der Mediator muss daher, wenn er den Medianden die Einwahldaten zur Videokonferenz übersendet, sicherstellen, dass er die aktuellen und korrekten Email-Adressen verwendet. Ggf. kann hier bereits die Frage der Verschlüsselung der Kommunikation gestellt werden[143].

Sofern das eingesetzte Tool keine personalisierten Einwahldaten für die Teilnehmer sondern generische Weblinks vorsieht, ist der Mediator aufgerufen, gleich mit der Einladung die Parteien darauf hinzuweisen, dass der Link nicht weitergeleitet oder mit anderen Personen geteilt werden darf. Für den Fall, dass die Teilnahme Dritter einvernehmlich von allen beschlossen wurde, sollte der Mediator selbst die Einladung diesen Dritten zusenden.

Ein weiterer Sicherheitsaspekt besteht in der Wahl der Konferenzbezeichnung. So, wie bei einer Anmietung von kommerziellen Räumen für Mediationen der Titel die Parteinamen und den Begriff „Mediation“ nicht enthalten sollte[144], sollten für

[143] Im Detail hierzu unten in Abschnitt 7.5.3.

[144] Anders im Beispiel von Duve/Eidenmüller/Hacke, S. 120.

Videokonferenzen ebenfalls neutrale Titel gewählt werden. Sofern nur generische, zufällig erstellte und vom Anbieter vorgeschlagene Zeichenfolgen verwendet und im Link eingebettet werden, ist es unwahrscheinlich, dass Dritte dies erraten und die Konferenz mittels „Zoombombing" stören[145]. Insbesondere wenn ein Konferenzraum mehrfach genutzt werden soll, empfiehlt sich darüber hinaus die Verwendung einer PIN oder Passwortkennung, die den Beteiligten separat mitgeteilt wird, und für deren Verwaltung besondere Sicherheitsregelungen gelten[146]. Bietet das ausgewählte Konferenztool die Möglichkeit automatischer Eintragung im Terminkalender, sollte der Mediator selbst die Konferenzdaten nur in einem geschützten Kalender eintragen und die Parteien darauf hinweisen, dass diese Funktion zum Schutz vor Öffentlichkeit nur zur Verwendung in Kalendern geeignet ist, auf die keine unbefugten Dritten zugreifen können[147].

6.1.2. Eröffnung

Vor Ort lässt der Mediator nur die Parteien und zugelassene Dritte in den Besprechungsraum ein. Als Organisator der Videokonferenz hat er demgemäß dafür zu sorgen, dass im ersten Schritt nur solche Personen an der Konferenz teilnehmen, die auch eingeladen worden sind. Hierzu sollte in jedem Fall in der Konferenzeinrichtung ausgewählt werden, dass vor dem Moderator keine Teilnehmer den virtuellen Konferenzraum betreten – sonst müsste der Mediator unmittelbar nach seinem eigenen Zutritt zunächst die bereits Anwesenden prüfen und ggf. entfernen.

Am besten wird die Zutrittssicherung bei der Eröffnung über einen sog. Warteraum („Waiting Room") erreicht. Diese Funktionalität ist eine bei der Organisation der Konferenz wählbare Option bei vielen Anbietern und mitunter auch als Standard voreingestellt. Sie bewirkt, dass die Teilnehmer nach dem Click auf den Link nicht direkt der Konferenz beitreten, sondern in einer virtuellen Rezeption landen und in der Konferenz der Einlasswunsch in einem Popup-Fenster angezeigt wird. Der Mediator kann dann in der Rolle des Videokonferenzmoderators den Zutritt gewähren.

---

[145] Mit „Zoombombing" wird das unbefugte Betreten eines Videokonferenzraums bezeichnet, das in der Anfangszeit vor allem im Kontext des Dienstanbieters Zoom auftrat: Fremde Personen errieten die Sitzungsbezeichnung einer laufenden Zoom-Konferenz, traten ihr unbefugt bei und überschwemmten den Chat oder auch den geteilten Bildschirm mit unangemessenen Inhalten – siehe bspw. die Kurzmeldung unter https://www.baden-wuerttemberg.datenschutz.de/virtuelle-konferenz-ueber-zoom-online-schulstunde-an-freiburger-gymnasium-gehackt/ (Der dort ursprünglich verlinkte Bericht des SWR ist nur noch über Archive erreichbar, bspw. über https://web.archive.org/web/20210225201227/https://www.swr.de/swraktuell/baden-wuerttemberg/suedbaden/online-schulstunde-zoom-gehackt-gymnasium-freiburg-100.html).

[146] BSI Kompendium VK 4-2020, S. 91f.

[147] BSI Kompendium VK 4-2020, S. 89.

Diese Funktion sollte beim Aufsetzen der Konferenz der Moderatorenrolle vorbehalten bleiben. Für aufwändigere Verfahren bietet es sich für den Mediator an, eine zweite Person mit dieser Aufgabe zu betrauen. Hierzu sollte ein Videokonferenzdienst ausgewählt werden, der neben dem Organisator der Konferenz weitere Personen mit administrativer Rolle zulässt. Und schließlich bieten manche Konferenzanbieter eine Zwei-Faktor-Authentifizierung an, bei der die Identität jedes Teilnehmers zusätzlich zum Aufruf des Links auf dem Endgerät über einen mittels SMS versendeten Einzelfall-Code verifiziert wird, der beim Zutritt eingegeben werden muss. Soweit es im Videodienst – insbesondere bei solchen, die Benutzerkonten vorsehen – möglich ist, sich selbst einen „Alias" (also eine gewählte Teilnehmerbezeichnung) zu geben, sollte der Mediator die Teilnehmer darum bitten, dass hier die Klarnamen verwendet werden.

Manche Dienste, wie der bereits erwähnte sichere-videokonferenz.de, haben dagegen keinen Warteraum, mit dem die Teilnehmer gezielt eingelassen werden könnten. Auch ist – obwohl der Mediator den Link auf der Webseite ursprünglich generiert hat – damit nicht automatisch eine Moderatorenrolle verbunden. Derjenige, der über den Klick auf den Link den Konferenzraum als erster betritt, ist automatisch „Moderator" und hat alle administrativen Rechte, bis er sie einem anderen Teilnehmer überträgt. Der Mediator muss daher in der Praxis bei diesem Anbieter darauf achten, dass er vor den Parteien im Konferenzraum ist, um Rollen-Missverständnisse zu vermeiden.

6.1.3. Durchführung

Wie bei der Begrüßung in der Mediation vor Ort, empfiehlt es sich – bei einer geringen Anzahl von Teilnehmern – zur Verifikation der Identität zu Beginn alle um eine kurze Vorstellung bei eingeschalteter Kamera zu bitten. Für die Zwecke der Mediation ist es – wie in Abschnitt 2.3 beschrieben – hilfreich, wenn die Videoübertragung jedes Teilnehmers grundsätzlich während der Dauer des Verfahrens eingeschaltet bleibt. Nur dann ist eine der physischen Präsenz zumindest ähnliche Kommunikationsreichhaltigkeit gegeben. Sollte es dennoch notwendig sein, vorübergehend das Video einzelner Personen anzuhalten, sei es, weil der Fokus ausschließlich auf dem Sprecher liegen soll (bei der Zuschaltung eines beratenden Experten), oder weil bspw. eine Partei einen Moment der Privatheit benötigt, ist in den Einstellungen der Konferenz (sofern im konkreten Dienst vorgesehen) darauf zu achten, dass diese Teilnehmer ohne Videoübertragung weiterhin als Anwesende auf dem Bildschirm angezeigt werden und nicht ausgeblendet werden, sonst gehen sie in der Übersicht verloren.

Um auszuschließen, dass sich unbefugt weitere Personen in den von den Parteien zur Teilnahme an der Videokonferenz gewählten Räumlichkeiten physisch aufhalten, kann theoretisch jeder Teilnehmer gebeten werden, durch einen Kameraschwenk einen Blick in den Raum zu ermöglichen[148]. Dies ist jedoch ein sehr weitgehender Eingriff in die Privatsphäre und daher nur ratsam, wenn entweder konkrete Anhaltspunkte für die Anwesenheit Unbefugter sprechen, oder aufgrund des Themas eine besondere Vertraulichkeit geboten ist. Im Normalfall sollte es ausreichen, die Parteien daran zu erinnern, dass außer den Eingeladenen niemand im selben Raum teilnehmen oder zuhören darf.

Sind alle Teilnehmer beigetreten, muss – wie durch das Schließen der Besprechungsraumtür vor Ort – auch die Konferenz gegen den nachträglichen Zutritt Unbefugter geschützt werden. Dies wird – insbesondere wenn ein Warteraum fehlt – über ein nachträgliches Passwort erreicht.

Bei größeren Teilnehmerzahlen ist es hilfreich, über die i. d. R. vorhandene Teilnehmerliste zu Beginn und regelmäßig im Verlauf der Konferenz zu prüfen, wer eingewählt ist. Diese Teilnehmerliste schafft – gerade bei einer Vielzahl von Parteien in Großverfahren – die nötige Übersicht, die bei einer Darstellung aller Teilnehmer als „Kacheln" auf dem Bildschirm verloren gehen kann. Dazu kann sich die Teilnehmerliste in diesen Fällen dauerhaft im Vordergrund des Bildschirms befinden[149]. Personen, die trotz der gewählten Sicherheitsmerkmale unbefugt beigetreten sind, können auf diese Weise vom Mediator entfernt werden[150].

Nach Unterbrechungen und geplanten Pausen, in denen die Konferenz beendet oder zumindest die Video- und Tonübertragung ausgeschaltet war, ist es u. U. ratsam, dass der Mediator die Identität der Teilnehmer erneut verifiziert.

Und schließlich ist die Videokonferenz gegen Abhören oder Kenntnisnahme Unbefugter zu schützen. Dieses Risiko ähnelt der Gefahr bei der Mediation vor Ort, dass Personen außerhalb des Besprechungsraums vom Inhalt des Mediationsgesprächs Kenntnis erlangen. Die Möglichkeiten unbefugten Abhörens sind jedoch bei der Online-Mediation aufgrund der technischen Gegebenheiten ungleich größer:

Insbesondere das eingesetzte öffentliche Telekommunikationsnetz bietet in vielfacher Hinsicht Angriffsmöglichkeiten auf die für die Videokonferenz notwendige Datenübertragung. Außerdem werden Daten auf den Servern des Anbieters und auf

---

[148] Gläßer/Sinemillioglu/Wendenburg ZKM 2020, 80, 83.
[149] BSI Kompendium VK 4-2020, S. 92.
[150] BSI Kompendium VK 4-2020, S. 91f.

den vermittelnden Servern unterwegs zum Transportzweck notwendigerweise technisch zwischengespeichert. Und schließlich liegen ggf. während der Konferenz entstandene Chatverläufe für die Dauer der Konferenz gespeichert auf den Anbieter-Servern.

Neben den bereits beschriebenen Maßnahmen zum Schutz der Konferenz selbst sollte daher eine Verschlüsselung erwogen werden. Da dieses Thema überwiegend im Kontext Datenschutz behandelt wird, stellt die vorliegende Arbeit die Erwägungen hierzu auch weiter unten in Abschnitt 7.5.3 vor.

6.1.4. Ende der Videokonferenz

Beim Beenden der Konferenz hat der Mediator darauf zu achten, dass er nicht nur selbst die Konferenz verlässt, sondern diese auch für alle Teilnehmer beendet. Andernfalls besteht der virtuelle Raum – ohne seine Kontrollmöglichkeit – fort und wird in seiner Abwesenheit u. U. von Dritten betreten. Für die Dauer der Konferenz gespeicherte Inhalte sollten vom Anbieter nach dem Ende der Konferenz automatisch gelöscht werden.

6.2. Verschwiegenheitspflicht des Mediators

Wie bei der Vor-Ort-Mediation auch, bedeutet die Verschwiegenheitspflicht in Bezug auf Mediationen in Videokonferenzen für den Mediator, dass er die Mediationsinhalte, d. h. bei der Videokonferenz die Gespräche, Videoeindrücke und insbesondere während der Konferenz entstandene Chatverläufe und andere Inhalte sowie überlassene Dokumente unbefugten Dritten nicht mitteilen oder zugänglich machen darf.

Neben den im Rahmen der Nichtöffentlichkeit beschriebenen Schutzmaßnahmen ist daher insbesondere Wert auf die **geschützte Speicherung** der Chatverläufe und der ggf. gemeinsam während der Konferenz erstellten Inhalte (bspw. auf virtuellen Whiteboards) zu legen. Hierzu enthalten die Verträge der Anbieter entsprechende Vertraulichkeitspflichten, nach denen sie a) auf die gespeicherten Inhalte nicht unbefugt zugreifen und b) sie nach dem Ende der Videokonferenz löschen müssen[151]. Insbesondere wenn im Rahmen der Mediation mehrere Sitzungen in

[151] Siehe zur Vertraulichkeit im Kontext des Datenschutzes in den folgenden in **Anhang 4** aufgeführten Beispielen von Auftragsverarbeitungsvereinbarungen jeweils: alfaview AVV § 10 u. Anlage 1; Microsoft DPA S. 11 u. S. 19; sichere-videokonferenz.de AVV Ziff. 4 (3) u. (4), und Ziff. 11; Wire AVV Ziff. 3.2, 5.1 u. 7.1; Zoom DPA Ziff. 3.4, 4, 5.4, 6.2.2.

Folge über Videokonferenz stattfinden, kann auch die Aufbewahrung für Chatverläufe und ggf. am virtuellen Whiteboard gemeinsam erarbeiteter Inhalte gewünscht sein, sowie bei Mediationen vor Ort ggf. auf Wunsch der Parteien erstellte Flipchart-Aufschriebe oder Dokumentationen aufgehoben werden sollen. In diesem Fall sollte der Mediator mit den Parteien besprechen, wo diese elektronischen Inhalte verwahrt werden. Dies ist – bei entsprechender Zusatzfunktionalität – beim Dienstanbieter durch zentrale Speicherung möglich und sollte dort ebenfalls geschützt sein[152]. Alternativ lädt der Mediator diese Inhalte jeweils auf sein Endgerät herunter und verwahrt sie dort vertraulich bis zur nächsten Konferenz.

Soweit die Mediationsordnung bzw. Vereinbarung mit den Parteien auch die Existenz des Verfahrens und die Identität der Medianden[153] in die Verschwiegenheitspflicht einbezieht, kann dies bereits durch die Organisation einer Videokonferenz gefährdet werden: Die Parteien melden sich in identifizierbarer Weise bei der Konferenz an, oder haben sogar Nutzerkonten angelegt. Hier ist in den Anbieterbedingungen darauf zu achten, dass derartige konferenzbezogene Nutzerdaten nur für die Zwecke der Konferenzorganisation verwendet werden, aber nicht zur wertschöpfenden Verknüpfung mit anderen Nutzerinformationen[154].

Manche Tools sehen die optionale **Aufzeichnung** der Videokonferenz, oder sogar die Erstellung eines Transkripts der Aufzeichnung vor (bspw. alfaview). Dies ist in der Regel bei Mediationen nicht ratsam[155], da es dem Vertraulichkeitsinteresse im Sinne der konstruktiven und offenen Gesprächsatmosphäre zuwiderläuft. Sollte dies ausnahmsweise zu Dokumentationszwecken einvernehmlich von den Parteien gewünscht werden, ist wie bei Chatverläufen eine geschützte Speicherung auf den Servern des Anbieters während der Dauer der Konferenz erforderlich[156]. Für die anschließende Aufbewahrung der erstellten Aufzeichnung sollten Mediator und Parteien vereinbaren, wo und in welcher Form die u. U. sehr großvolumigen Dateien abgelegt werden, um eine dem vereinbarten Zweck entsprechende Verwendung zu ermöglichen, aber den Zugriff Unbefugter auszuschließen. Sollte die eingesetzte Konferenzlösung im Standard eine Aufzeichnung vorsehen, ist diese Option vom Mediator beim Aufsetzen der Konferenz abzuwählen, es sei denn die Parteien haben ihn im Vorfeld anderweitig instruiert.

---

[152] Zur Verschlüsselung siehe Abschnitt 7.5.3.

[153] S. o. in Abschnitt 3.2.

[154] Siehe dazu im Kontext Datenschutz in Abschnitt 7.

[155] BMEV Knigge VK, S. 2.

[156] Zur Verschlüsselung s. u. Abschnitt 7.5.3.

So, wie für ausnahmsweise vereinbarte Einzelgespräche mit den Parteien bei der Vor-Ort Mediation getrennte Räume aufgesucht werden, sind während der Videokonferenz beim Einsatz von Konferenztools mit großem Funktionsumfang sog. „**Break-Out Rooms**" für definierte Teilnehmergruppen möglich. Der Mediator richtet sie als Konferenzmoderator ein, weist sie den Teilnehmern gezielt zu und betritt sie virtuell zur Gesprächsführung.

Über „**Screen-Share**" allen Teilnehmern virtuell geteilte Unterlagen verbleiben grundsätzlich technisch auf den Rechnern des jeweils Teilenden, werden aber für die Dauer des Bildschirmteilens im Rahmen der Videokonferenz allen Teilnehmern – wie auch die Audio- und Videoinhalte – übermittelt. Für sie gilt das im Rahmen der Nichtöffentlichkeit der Konferenz in Abschnitt 6.1 Beschriebene.

Eine effiziente **Co-Mediation**[157], in der beide Mediatoren gleichberechtigt agieren, setzt ein identisches Informationsniveau bei beiden Akteuren voraus. Daher ist der Co-Mediation immanent, dass beide Mediatoren gleichermaßen Zugang zu den vertraulichen Informationen haben, auch soweit diese ggf. aus Einzelgesprächen mit den Parteien stammen[158] und entsprechend gleichermaßen zur Verschwiegenheit verpflichtet sind. Diese Möglichkeit des unbeschränkten Austauschs ist den Parteien zu Beginn der Mediation offenzulegen und mit ihnen im Mediationsvertrag zu vereinbaren, wenn in Break-Out-Rooms organisierte Einzelgespräche gewünscht sind.

Im Kontext der Verschwiegenheitspflicht des Mediators ist schließlich auf die Risiken hinzuweisen, die sich beim Einsatz von Videokonferenzanbietern ergeben, die ihren **Sitz außerhalb der EU** haben bzw. ihre Dienste nicht ausschließlich in Europa erbringen. Zwar ergeben sich aus dem Ordre Public Vorbehalt in § 4 S. 3 MediationsG, sowie durch den Vorbehalt abweichender gesetzlicher Regelung in § 4 S. 1 MediationsG Einschränkungen der Verschwiegenheitspflicht. Diese Ausnahmen fußen jedoch, ebenso wie die in Abschnitt 3.2 dargestellten unterschiedlichen Rechtsfolgen im Kontext geltender Prozessordnungen, auf den Grundwerten der für den Mediator geltenden lokalen Rechtsordnung in Deutschland[159] und basieren auf dem Überwiegen der jeweils vorrangigen Rechtsgüter[160]. Eine gewisse Harmonisierung der Werteordnung wird überdies in der EU durch die GRCh erreicht. Dienstanbieter außerhalb dieses geografischen Bereichs müssen demgegenüber gemäß dem für sie vor Ort geltenden nationalen Recht u. U. andere gesetzliche,

---

[157] Gläßer/Sinemillioglu/Wendenburg ZKM 2020, 80, 82.
[158] Haft/Schlieffen-*Hartmann* § 28 Rn. 8.
[159] Greger/Unberath/Steffek-*Greger* MediationsG § 4 Rn. 15.
[160] Haft/Schlieffen-*Hartmann* § 28 Rn. 23.

oder im Einzelfall behördlich oder gerichtlich angeordnete Herausgabepflichten für von ihnen gespeicherten oder vermittelten Daten erfüllen. Dieser Rechtskonflikt zwischen ausländischem Eingriffsrecht und europäischen Schutzrechtsvorschriften wird insbesondere im Kontext der Zulässigkeit internationaler Transfers personenbezogener Daten thematisiert und daher in der vorliegenden Arbeit zusammen mit den datenschutzrechtlichen Fragestellungen in Abschnitt 7.5 behandelt.

6.3. Vertraulichkeit zwischen den Parteien

Ebenso wie bei der Mediation vor Ort sollten auch im Kontext von Online-Mediationen die Vertraulichkeitspflichten zwischen den Parteien mangels gesetzlicher Regelung erörtert und zum Gegenstand einer expliziten Vertraulichkeitsabrede gemacht werden[161]. Der Mediator sollte mit den Parteien dabei die Besonderheiten bei der Durchführung per Videokonferenz erörtern, in Abhängigkeit von deren Erfahrung mit derartigen Kommunikationsmitteln.

Auch wenn die Parteien ihre Vertraulichkeitspflichten grundsätzlich in einer zweiseitigen Abrede selbst, d. h. ohne Mitwirkung des Mediators vereinbaren können[162], ist es – insbesondere, wenn der Mediator selbst das Konferenztool wählt – empfehlenswert, die Definition der konkreten Pflichten nicht allein den Parteien zu überlassen, da der Mediator die mit dem von ihm konkret gewählten Dienst einhergehenden Risiken oder Möglichkeiten besser überblickt. Daher empfiehlt es sich – insbesondere bei juristisch unerfahrenen Medianden – dass der Mediator hierzu ein standardisiertes Muster[163] vorhält.

Gegenstand der Vertraulichkeitspflichten ist – wie vor Ort – in erster Linie das **Gespräch** selbst[164]. Es wird aus Vertraulichkeitsgründen im Kontext der Mediation explizit von der Durchführung einer Aufzeichnung innerhalb des Konferenztools abgeraten[165], auch wenn diese Funktionalität vorhanden ist. Dies entspricht dem Interesse der Parteien an einer vertrauensvollen und damit konstruktiven Atmosphäre, bei der keine Seite befürchten muss, dass ihre Äußerungen bei Scheitern der Mediation oder schlicht außerhalb des geschützten Raums zweckentfremdet werden.

---

[161] Haft/Schlieffen-*Kracht* § 13 Rn. 124.

[162] Greger/Unberath/Steffek-*Greger* MediationsG § 4 Rn. 50 und im Detail zur Mediationsabrede und anderen vertraglichen Beziehungen Greger/Unberath/Steffek-*Greger* MediationsG § 1 Rn. 132ff., insbes. 142ff.

[163] Siehe die generellen Erwägungen und konkreten Beispiele und Vorschläge bei Greger/Unberath/Steffek-*Greger* MediationsG § 4 Rn. 52–60 sowie bei Troja ZKM 2009, 152, 156f.

[164] Greger/Unberath/Steffek-*Greger* MediationsG § 4 Rn. 54.

[165] BMEV Knigge VK, S. 2.

So, wie es vor Ort überdies unzulässig ist, heimliche **Aufzeichnungen** des Mediationsverfahrens z. B mit dem Smartphone anzufertigen, dürfen die übermittelten Audio- und Videodaten der Konferenz auch nicht heimlich am Bildschirm eines Teilnehmers aufgezeichnet werden. Gleiches gilt für Screenshots von geteilten Inhalten oder Copy-Paste-Kopien von Chatverläufen. Manche Tools bieten dabei eine automatische „Wasserzeichen"-Funktion als Absicherung gegen unbefugte Screenshots. Sie bewirkt, dass in der Screenshot-Datei automatisch die Nutzerkennung desjenigen eingeblendet ist, der den Screenshot an seinem Endgerät erstellt hat[166].

In der Praxis kann natürlich eine Aufnahme auch über ein **zweites Endgerät**, also bspw. über die Smartphone-Kamera, erfolgen. Auch dies ist unzulässig, es sei denn, die Parteien haben Abweichendes vereinbart.

Da mangels Anwesenheit der Parteien im selben Raum diese Vorgänge alle technisch möglich und dabei für die übrigen Teilnehmer nicht sichtbar sind, empfiehlt es sich, Regelungen hierzu explizit zu vereinbaren[167] und alle Beteiligten zu Beginn und ggf. im weiteren Verlauf der Konferenz hieran zu erinnern, um den für die konstruktive Konfliktbearbeitung erforderlichen sicheren Rahmen zu betonen.

Sollte das reine Gegenseitigkeitsprinzip der wechselseitig vertraglich aufeinander bezogenen Vertraulichkeitspflichten nicht zum Schutz ausreichen, weil bspw. die eine Seite Informationen von höherer Relevanz preisgibt, empfiehlt sich die Vereinbarung einer **Vertragsstrafe** für den Fall der Verletzung durch Verwendung vertraulicher Informationen[168].

---

[166] Siehe bspw. die Beschreibung der „Watermark"-Funktion bei Zoom, unter https://support.zoom.us/hc/en-us/articles/209605273-Adding-a-Watermark.

[167] Gläßer/Sinemillioglu/Wendenburg ZKM 2020, 80, 83.

[168] Haft/Schlieffen-*Kracht* § 13 Rn. 131ff.

7. Datenschutzrecht bei der Mediation über Videokonferenz

In einigen Einschätzungen zum Einsatz moderner Kommunikationsmittel findet sich die pauschale Bewertung, sie seien datenschutzrechtlich „kritisch“ [169], und stattdessen seien schlicht herkömmliche Telefonate und Telefonkonferenzen zu führen[170], weil für sie die Datenschutzkonformität leichter umzusetzen sei[171]. Dies ist allerdings gerade dann, wenn sich die Parteien wegen der höheren Reichhaltigkeit der Kommunikation für die Durchführung einer Videokonferenz entschieden haben, nicht sinnvoll.

Stattdessen ist konkret zu untersuchen, welche Gestaltungen in der Praxis möglich sind, welche Rollen und Aufgaben der Mediator, der Dienstanbieter und die Parteien haben, und welche Fragestellungen besondere Lösungen erfordern.

7.1. Verarbeitung personenbezogener Daten und Rechtsgrundlagen

Zunächst ist zu klären, wo überall beim Durchführen einer Mediation über Videokonferenz Verarbeitungen personenbezogener Daten stattfinden, und welche rechtlichen Grundlagen in Betracht kommen.

7.1.1. Verarbeitung personenbezogener Daten

Alle Angaben der Parteien zu ihrer Identität, die für die Kontaktaufnahme und Vertragsdurchführung erforderlich sind, sind als personenbezogene Daten schutzwürdig und insoweit Gegenstand einer datenschutzrechtlichen Verarbeitung durch den Mediator, als er den Parteien bspw. Emails schreibt oder elektronisch Rechnungen übermittelt. Auch die Einwahl der Parteien in die Konferenz über den vom Mediator zur Verfügung gestellten Link beinhaltet einen datenschutzrechtlichen Verarbeitungsvorgang, denn die dabei erfasste IP-Adresse des Endgeräts ist ein personenbezogenes Datum.

---

[169] So undifferenziert Schmidt-*Haschert* § 20 Rn. 137ff.

[170] BBDI Empfehlungen VK 03.07.2020, S. 3, und auch in der inzwischen nicht mehr abrufbaren Vorversion aus dem April 2020, kritisch kommentiert bei Piltz/Hessel, Reuschlaw-Blog 4-2020.

[171] BBDI Empfehlungen VK 03.07.2020, S. 3.

Ein wesentlicher Unterschied zur Durchführung der Mediation vor Ort besteht jedoch in Folgendem: Während vor Ort die Inhalte des Mediationsgesprächs und ihre Darstellung auf Flipcharts, die Falldokumentation auf Papier und selbst manuell geführte Akten nicht dem Datenschutzrecht unterliegen[172], sind bei Mediationen über Videokonferenz alle dabei entstehenden Audio- und Videodaten, d. h. mündliche Äußerungen aber auch Aussehen oder Mimik, ebenso wie Chatinhalte oder Visualisierungen am Bildschirm, von datenschutzrechtlichen Pflichten erfasst, da jeweils IT-gestützte Verarbeitungen vorliegen. Damit ist für diese Daten immer gem. Art. 2 Abs. 1 DSGVO der sachliche Anwendungsbereich des Datenschutzrechts eröffnet. Die Verarbeitung umfasst bei Videokonferenzen gem. Art. 4 Nr. 2 DSGVO insbesondere die Erhebung der Daten, ihre (vorübergehende) Speicherung, ihre Verwendung im Rahmen des Gesprächs, ihre Übermittlung im Rahmen der Konferenzdurchführung, sowie regelmäßig die Löschung am Ende der Konferenz.

7.1.2. Rechtsgrundlagen

Der Mediator verarbeitet die personenbezogenen Daten der Parteien bei der Durchführung der Mediation via Videokonferenz gemäß Art. 6 Abs. 1 lit. b DSGVO in **Erfüllung des Mediationsvertrages,** im Rahmen dessen die Videokonferenz vereinbart ist.

Auch für die personenbezogenen Daten **anderer Konfliktbeteiligter,** die im Kontext der Mediationsgespräche einbezogen werden, ist das Datenschutzrecht relevant. Für sie gilt Art. 6 Abs. 1 lit. b DSGVO nicht, denn sie sind nicht Vertragspartner der Mediationsabrede. Stattdessen kommt eine Rechtfertigung gemäß Art. 6 Abs. 1 lit. a DSGVO in Betracht, wenn und soweit die Parteien von diesen Personen im Vorfeld die Einwilligung einholen. Allerdings sind Gesprächsinhalt und Breite der Erörterung für die Parteien nicht vollständig vorhersehbar, und überdies würden die Parteien u. U. weitere Konfliktfelder eröffnen, wenn sie zunächst den Gegenstand der Mediation mit weiteren am Rande relevanten Personen besprächen, um deren Einwilligung zu erlangen. Stattdessen bietet sich eine Rechtfertigung über Art. 6 Abs. 1 lit. f DSGVO über das überwiegende berechtigte Interesse der Parteien an der Konfliktbearbeitung im Wege der Videokonferenz an, hinter dem die Interessen dieser übrigen Konfliktbeteiligten zurückstehen müssen. Dies kann jedoch wohl nur soweit reichen, wie sie Gegenstand der Gespräche sind. Die dauerhafte Aufnahme in Aufzeichnungen oder auch in dokumentierten Chat-Verläufen

[172] Ehmann/Selmayr-*Klabunde* Art. 4 Rn. 35; anders Bertolino ZKM, 58, 58.

greift hingegen deutlich weiter in das Recht dieser Personen ein und sollte daher nur mit vorheriger Einwilligung erfolgen. Dies ist ein weiterer Grund, von Aufzeichnungen im Rahmen von videokonferenzbasierten Meditationen grundsätzlich abzusehen.

7.2. Betrieb auf eigener Infrastruktur

Mehrere Datenschutzaufsichtsstellen haben eine ausdrückliche Empfehlung für den eigenen Betrieb von Videokonferenz-Software auf eigenen Servern ausgesprochen, da nur dort Datenflüsse selbst kontrolliert werden könnten und eine Übertragung oder Speicherung personenbezogener Daten (sowohl Metadaten über die Verbindung und ihre Teilnehmer sowie Inhaltsdaten der Kommunikation) durch Dritte ausgeschlossen seien[173].

Kann dies von einem Mediator gefordert werden, der einen Videokonferenzdienst zum Zweck der Durchführung der Mediation einsetzen möchte? Und ist (nur) diese Betriebsart hinreichend sicher, datenschutzrechtlich zulässig und dem Interesse der Betroffenen an informationeller Selbstbestimmung angemessen?

Die Regelungen des Datenschutzrechts fordern und erlauben eine risikobasierte Herangehensweise, die mittels einer Interessen- und Rechtsgüterabwägung zu erfolgen hat[174]. Zur Erfüllung der DSGVO-Pflichten geeignete technische und organisatorischen Maßnahmen (also auch Auswahl und Einsatz von IT-Infrastruktur) hat der Mediator als Verantwortlicher gemäß Art. 24 Abs. 1 DSGVO insbesondere anhand der Risiken für die personenbezogenen Daten entsprechend der Art und der konkreten Verarbeitungsweise und -zwecke zu bestimmen. Hierbei ist der Stand der Technik zu berücksichtigen. Gemäß Artt. 25 Abs. 1 und 32 Abs. 1 DSGVO fließt in die Abwägung jedoch auch der Implementierungsaufwand für den Verantwortlichen ein.

Zum einen bieten selbst-betriebene Konferenzanwendungen zwar größere Konfigurationsmöglichkeiten in Bezug auf datenschutzrelevante Einstellungen[175], d. h.

---

[173] BBDI Empfehlungen VK 03.07.2020, S. 3f.; BBDI Hinweise VK 18.02.2021, S. 1.; LfD BW Datenschutzfreundliche Kommunikation 17.04.2020; DIHK Alternativen zu Videokonferenz 30.03.2020, auch auf den Empfehlungsseiten des BMEV verlinkt; DSK OH VK 23.10.2020, S. 5 und BRAK Hinweise VK 07.01.2021.

[174] Dendorfer-Ditges/Schmidt-Gorbach KD 2018, 318, 325.

[175] John/Wellmann DuD 2020, 506, 507.

es sind bedarfsgerechtere und datenschonendere Optionen wählbar[176], und der Mediator behält als Betreiber in der Tat die vollständige Kontrolle über das, wofür er als Verantwortlicher einsteht.

Zum anderen wird zu Recht darauf hingewiesen, dass der eigene Betrieb nicht pauschal als „datenschutz-konform" bezeichnet werden kann, sondern immer eine aufwändige Konfiguration voraussetzt, die im Zweifel IT-Fachpersonal überlassen bleiben sollte[177]. Die Einrichtung und der Unterhalt einer eigenen IT-Infrastruktur für Videokonferenzen sind für kleinere Mediationsbüros oder Einzelmediatoren kaum leistbar[178]. Sie bleiben bei der weiteren Betrachtung daher außen vor.

Stattdessen liegt der Fokus vorliegend auf dem Einsatz von Videokonferenztools, die als „Software-as-a-Service"-Lösung über das Internet bereitgestellt und vom Mediator genutzt werden.

7.3. Einschub Telekommunikationsrecht

Der Mediator kann sich – de lege lata – gegenüber dem Videokonferenzanbieter nicht auf das für den Internetanschluss geltende Fernmeldegeheimnis und die gesetzlichen Datenschutzregelungen des TKG berufen[179], sondern ist auf die Regelungen der DSGVO angewiesen:

Mangels eindeutiger rechtlicher Begriffsdefinitionen bereits im europäischen Primärrecht[180] und begünstigt durch die Tatsache, dass herkömmliche leitungsbasierte Text- und Sprachübermittlungsdienste (wie SMS und Telefonie) zunehmend durch Leistungen im Internet ersetzt werden[181], wird zwar seit längerem diskutiert[182], ob und ggf. in welchem Umfang Telekommunikationsrecht auch auf sog. Over-the-Top Kommunikationsdienste (OTT-1 Dienste)[183], also insbesondere

[176] DSK OH VK 23.10.2020, S. 5f.
[177] Ertel Blog 14.05.2020.
[178] BBDI Empfehlungen VK 03.07.2020, S. 3; DSK OH VK 23.10.2020, S. 6.
[179] BBDI Hinweise VK 18.02.2021, S. 2.
[180] Simitis/Hornung/Spiecker-*Karg* Art. 95 Rn. 5.
[181] Kiparski CR 2019, 460, 460.
[182] Zum Streitstand bereits Sassenberg/Franke CR 2013, 772ff. und Kühling/Schall CR 2015, 641ff. m. w. N., allerdings in Teilen von der Rechtsprechung inzwischen überholt.
[183] WAR-Stellungnahme 2013, S. 1f.; Kühling/Schall CR 2015, 641, 642.

Chat-, Internettelefonie-, Videokonferenz- oder sonstige internetbasierten Kommunikationsdienste anzuwenden sind[184].

Das Nebeneinander von DSGVO und TKG führt zu Rechtsunsicherheiten nicht nur bei den Nutzern derartiger Dienste, sondern auch bei ihren Anbietern und bei den Aufsichtsbehörden. Die Schaffung eines einheitlichen europäischen Rechtsrahmens für die Anbieter von internetbasierten Kommunikationsleistungen durch die geplante ePrivacy-VO und die Umsetzung des bereits in Kraft getretenen EECC in den Mitgliedsstaaten, ist jedoch abzuwarten[185].

Derzeit werden zwei gesetzgeberische Entwürfe zum TKG und zum TTDSG debattiert, in denen die Vorbereitung der nationalen Rechtslage auf diese europarechtlichen Änderungen beschrieben werden[186]. Ihr Inkrafttreten war usprünglich zum Ende des Jahres 2020 geplant und steht nun wohl zum Jahresende 2021 an. Die Kritik der Industrieverbände und des BMJV an weitgehenden regulatorischen Eingriffen in die sonstige Vertragsfreiheit der Telekommunikationsanbieter ist allerdings vielgestaltig[187]. Überdies wird der telekommunikationsspezifische Datenschutz maßgeblich durch die noch nicht verabschiedete, und jetzt neuerlich verzögerte[188] ePrivacy-VO bestimmt werden, so dass auf Bundesebene auch nach der Verabschiedung des TTDSG noch weitere Anpassungen folgen werden. Das Gesetzgebungsverfahren für beide Gesetze ist noch nicht abgeschlossen[189]. Im Vorliegenden wird daher von der Anwendung der DSGVO auf Videokonferenzdienste ausgegangen.

---

[184] Siehe dazu das Anmeldeformular der BNetzA unter https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Anbieterpflichten/Meldepflicht/Meldeformular_pdf.pdf?__blob=publicationFile&v=16 und bereits im Detail die Begründung der Bundesnetzagentur in der WAR-Stellungnahme aus dem Jahr 2016, sowie die DAV-Stellungnahme TKG (2013), S. 5ff. unter Hinweis auf den Regelungsbedarf de lege ferenda auf S. 7ff.

[185] Sehr kritisch der Beitrag von Engeler/Felber ZD 2017, 251ff.

[186] Ausgangspunkt der aktuellen Debatte waren der TKMoG-RefE, der zunächst unter https://netzpolitik.org/2020/so-soll-das-recht-auf-schnelle-internetanschluesse-aussehen/#TKMoG-Referentenentwurf „geleaked" wurde, sowie der TTDSG-RefE unter https://www.heise.de/downloads/18/2/9/4/6/4/2/1/20200731_RefE_TTDSG_cleaned.pdf. Dazu die Stellungnahmen von Kiparski in CR-online.de Blog 06.08.2020 und CR-online.de Blog 23.08.2020.

[187] Briegleb heise.de 27.10.2020; Krempl heise.de 20.11.2020; siehe auch die öffentliche Anhörung des Bundestags am 01.03.2021, unter https://www.bundestag.de/dokumente/textarchiv/2021/kw16-de-telekommunikationsmodernisierungsgesetz-834820.

[188] Krempl heise.de 20.11.2020.

[189] Siehe den Status bei Krempl heise.de 22.04.2021, ders. heise.de 07.05.2021 und im Abkürzungsverzeichnis/Glossar.

7.4. Einsatz eines Videokonferenzanbieters als Auftragsverarbeitung

Nutzt der Mediator das internetbasierte Angebot eines Videokonferenzanbieters, agiert er im Sinne der DSGVO als datenschutzrechtlich **Verantwortlicher** i. S. d. Art. 4 Nr. 7 DSGVO, da er – auch wenn er die Infrastruktur nicht selbst betreibt – dennoch die Entscheidungshoheit über die Zwecke und Mittel der Verarbeitung personenbezogener Daten hat[190] und insoweit rechenschaftspflichtig[191] bleibt.

Dem Dienstanbieter kommt dabei die Rolle als **Auftragsverarbeiter** gemäß Art. 4 Nr. 8 DSGVO zu[192], denn er ist rechtlich selbständig, d. h. nicht in die Organisation des Mediators als Verantwortlichem eingegliedert[193], und er ist mit der Verarbeitung personenbezogener Daten nach dessen Weisungen bei der Durchführung der Videokonferenz betraut[194]. Eine gemeinsame Verantwortlichkeit des Mediators und des Dienstanbieters gem. Art. 26 DSGVO scheidet mangels vollständig gleichförmiger Interessen in Bezug auf Verarbeitungszwecke aus[195].

7.4.1. Erforderlichkeit

Da der Einschaltung dieses weiteren Verarbeiters das Risiko der Verringerung des Schutzniveaus für die personenbezogenen Daten immanent ist[196], treffen beide Akteure besondere Pflichten zum Schutz der Interessen der Betroffenen, auf die im Folgenden näher einzugehen ist.

Für die Zwecke der vorliegenden Arbeit wird zur Veranschaulichung und Validierung der rechtlichen Anforderungen an geeigneten Stellen auf die von Datenschutzbehörden empfohlenen internetbasierte Dienste[197] (insbes. Netways Web Services, Jitsi Meet, Big Blue Button, sichere-videokonferenz.de, Wire[198] und

---

[190] Simitis/Hornung/Spiecker-*Petri* Art. 4 Nr. 7 Rn. 13ff.
[191] Simitis/Hornung/Spiecker-*Roßnagel* Art. 5 Rn. 174.
[192] LfD Nds FAQ 8-2020, S. 4; BBDI Empfehlungen VK 03.07.2020, S. 1f.
[193] Art. 29-DSG, WP 169, S. 30.
[194] EDSA Leitlinien 07/2020, S. 3. und S. 24ff.
[195] John/Wellmann DuD 2020, 506, 508f.
[196] Art. 29-DSG, WP 169, S. 30.
[197] Tixeo Cloud bleibt aufgrund seiner Preisstruktur außen vor, siehe https://www.tixeo.com/visioconference-securisee/solutions/service-de-visioconference-tixeocloud/. NextCloud Talk befindet sich zwar auch auf diesen Listen, setzt aber einen eigenen Betrieb voraus.
[198] BBDI Empfehlungen VK 03.07.2020, S. 4; LfDI BW PM 17.04.2020; Digitalcourage Blog 28.04.2020.

TeamViewer[199]), sowie auf die in der Praxis weitverbreiteten Dienste Zoom, GoogleMeet und Microsoft Teams exemplarisch eingegangen[200].

Bei der Auswahl des Dienstes sollte der Mediator i. S. d. **Datensparsamkeit** gem. Art. 5 Abs. 1 lit. c DSGVO im Rahmen des **Datenschutzes durch Technikgestaltung (Data Protection by Design)** gem. Art. 25 Abs. 1 DSGVO prüfen[201], welche Funktionen für den konkreten Mediationszweck erforderlich sind. Es empfiehlt sich dabei eine strukturierte Vorgehensweise nach dem MoSCoW-Prinzip[202]:

- **M**ust-have: Funktionalitäten, die unbedingt erforderlich sind, also bspw. die zuverlässige Übertragungsqualität für Audio- und Videostream;
- **S**hould-have: Funktionen, die die Effizienz erhöhen, die aber nicht notwendig sind, wie bspw. eine zusätzliche Moderatorenrolle für Co-Mediation oder bspw. eine Chat-Funktion, falls bei einer Person die Audio-Übertragung ausfällt;
- **C**ould-have: darüber hinaus gewünschte Features, wie bspw. Screen-Share, aber u. U. auch Aufzeichnung, falls gewünscht;
- **W**on't have: Funktionen, die aus rechtlichen oder praktischen Gründen derzeit (noch) nicht wirklich realisierbar sind, bspw. ein simultanes Dolmetschen der Äußerungen beider Seiten im Falle von Sprachbarrieren[203].

Diese Prüfung sollte in Abwägung zum mediativen Zweck des Einsatzes erfolgen[204] und kann sich an der Checkliste in **Anhang 1** orientieren.

Für wenig komplexe Konfliktthemen oder auch technisch nicht affine Medianden bietet sich u. U. eine einfache, kostenlose, über den Webbrowser nutzbare Konferenzlösung ohne Zusatzfunktionen an, die im Interesse der Parteien und des Mediators an einer reichhaltigen Kommunikation eine lediglich eine unterbrechungsfrei funktionierende Ton- und Bildübertragung gewährleisten muss. Als Dienste

---

[199] DIHK Alternativen zu Videokonferenz 30.03.2020.

[200] Eine überblicksartige datenschutzrechtliche Bewertung findet sich u. a. bei BBDI Hinweise VK 18.02.2021.

[201] John/Wellmann DuD 2020, 506, 507; GDD Praxishilfe DS-GVO XVI 4-2020, S. 6 dort als „Privacy by Design & by Default" bezeichnet.

[202] GDD Praxishilfe DS-GVO XVI 4-2020, S. 4.

[203] Microsoft Teams bietet über Microsoft Translator eine eingebettete, optionale, maschinelle Simultanübersetzung an. Eine Beschreibung findet sich hier: https://www.microsoft.com/de-de/translator/education/microsoft-teams-multilingual-meeting/.

[204] GDD Praxishilfe DS-GVO XVI 4-2020, S. 5.

kommen hier insbesondere sichere-videokonferenz.de und grundsätzlich weitere öffentliche Instanzen von Jitsi oder BigBlueButton in Betracht[205].

Bei komplexeren Konfliktbearbeitungen können dagegen zusätzliche Funktionen wie Screen-Sharing, Chat-Funktion, Co-Moderation, Umfragen (Polling), Handheben oder sogar Aufzeichnungen erforderlich sein, die in der Regel bei Anbietern komplexerer Tools wie alfaview, GoogleMeet, Microsoft Teams, Wire oder Zoom vorhanden sind. Des Weiteren ist für die Auswahl des Dienstes entscheidend, wie viele Personen sich einwählen werden. Manche Videodienste haben eine vereinbarte Obergrenze oder es zeigt sich zumindest in der Praxis, dass sie mitunter ab 8–10 eingewählten Anschlüssen nicht mehr zuverlässig und stabil laufen.

Des Weiteren muss der Dienst dem Grundsatz des **Datenschutzes durch Voreinstellung (Data Protection by Default)** gem. Art. 25 Abs. 2 DSGVO genügen, d. h. die Datenverarbeitung ausschließlich auf das zur Zweckerreichung Erforderliche beschränken. Mustergültig ist dies umgesetzt bei schlichten Videodienstlösungen, wie bspw. sichere-videokonferenz.de. Dienste, die dieses Kriterium nicht erfüllen und daher hier im Folgenden außer Betracht bleiben, sind bspw.[206]:

- **GoogleMeet:** Die allumfassende Datenschutzvereinbarung[207] der Fa. Google LLC mit Sitz in den USA listet auf mehreren Seiten (S. 3ff.) beispielhaft eine Vielzahl von Datenerhebungen und -verarbeitungen zu ebenfalls nicht abschließend beschriebenen Anbieter-eigenen Zwecken auf, die nur im Sinne eines Opt-Out in einer sehr unübersichtlichen Nutzerprofil-Verwaltung[208] abgestellt werden können. Des Weiteren weist Google im Rahmen der erlaubten Weitergabe von Daten an Partnerfirmen selbst auf die Verknüpfung zu „über zwei Millionen

---

[205] Siehe auch die Liste der Betreiber unter Digitalcourage Blog 28.04.2020.

[206] Auch in Bezug auf Microsoft Produkte wird dies mitunter kritisch bewertet: Der DSMV hat im März 2021 die Landesregierung von Mecklenburg-Vorpommern aufgefordert, aufgrund „rechtsgrundloser Datenabflüsse" u. a. die Nutzung von Microsoft Produkten einzustellen, siehe Pressemeldung https://www.datenschutz-mv.de/presse/?id=168438&processor=processor.sa.pressemitteilung. Zu einer vergleichbaren Einschätzung gelangte auch der LfDI BW Anfang Mai 2021 nach einem pilotierten Einsatz von Microsoft Produkten in Schulen, siehe dazu LfDI BW PM 07.05.2021; siehe auch Wilkens heise.de 07.05.2021.

[207] Siehe unter https://www.gstatic.com/policies/privacy/pdf/20200930/r9u74aii/google_privacy_policy_de_eu.pdf.

[208] https://myaccount.google.com/privacycheckup?utm_source=pp&utm_medium=Promo-in-product&utm_campaign=pp_intro&pli=1. Die dort angezeigte Webseite enthält aber bereits Voreinstellungen auf der Basis der Analyse der vom konkreten Nutzer meistgenutzten Google Services. Dies umfasst bspw. den Standort-Verlauf (Google Maps App auf dem Handy) und die Nutzung des Dienstes Youtube.

Webseiten und Apps“ hin, die „mit Google zu Werbezwecken zusammenarbeiten“[209]. Und schließlich erschafft Google nach der umfassenden Datenerhebung mittels strukturierter Verarbeitung zwischen Daten aus un-terschiedlichen Quellen eine Vielzahl von Querverbindungen, die die Daten zweckentfremden und letztlich zu einem Nutzerprofil führen, das dieser zwar mit Datenschutzeinstellungen beeinflussen und nach Artt. 13 u. 14 DSGVO auch über Auskunftsansprüche ausleuchten kann, das er in seiner gesamten Tragweite jedoch nicht mehr umreißen wird[210]. Bereits das BVerfG wies in seinem Urteil knapp vierzig Jahren auf den sog. „Chilling Effekt“ hin: „Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen. […]“[211].

- **NetWays** (empfohlen): Die Bedingungen der Fa. Netways GmbH mit Sitz in Deutschland[212], erlauben umfangreiche Datenweitergaben an Dritte, wie Twitter, Google oder Facebook[213] und
- **TeamViewer Blizz** (empfohlen): Für seinen Videokonferenzdienst weist der Anbieter Fa. TeamViewer Germany GmbH darauf hin, dass insbesondere Google Analytics und Social Media Tracking Tools (abseits des Vertragszwecks) eingesetzt werden[214].

Dem Mediator obliegt als Verantwortlichem in diesem Kontext insbesondere die Pflicht zur gebotenen Sorgfalt bei der **Auswahl des Anbieters** gemäß Art. 28 Abs. 1 DSGVO. Er hat hiernach, gemäß dem Schutzzweck der DSGVO für die Interessen der Betroffenen im Hinblick auf ihre informationelle Selbstbestimmung und Privatautonomie, insbesondere die Rechtmäßigkeit der vorgesehenen Verarbeitung personenbezogener Daten zu prüfen, und zu evaluieren, ob der Anbieter hierzu und insbesondere zum Schutz der Rechte der Betroffenen hinreichende Garantien sowie entsprechende technische und organisatorische Maßnahmen ergreift. Dem

---

[209] https://policies.google.com/privacy/google-partners.

[210] Einige Beispiele nennt Kuketz Blog 16.04.2019 m. w. N. allerdings aus dem Jahr 2018.

[211] BVerfGE 65, 1, 43 Rn. 146.

[212] https://nws.netways.de/de/.

[213] Ziff.13 der Datenschutzbedingungen unter https://www.netways.de/rechtliches/datenschutz/.

[214] Siehe Abschnitt E der General Privacy Policy unter https://www.teamviewer.com/en-us/privacy-policy/#website-web-analytics.

Mediator werden insoweit als Verantwortlichem die Verarbeitungstätigkeiten, die der Auftragsverarbeiter für ihn vornimmt, zugerechnet[215].

Für die Übertragung der Daten an den Auftragsverarbeiter ist aus diesem Grund keine gesonderte Rechtsgrundlage erforderlich. Die ursprüngliche Legitimierung der Verarbeitung, im vorliegenden Fall also gem. Art. 6 Abs. 1 lit. b und lit. f bzw. lit. a DSGVO, schließt sie mit ein[216].

7.4.2. Auftragsverarbeitungsvereinbarung

Zur Umsetzung der Pflichten zwischen Verantwortlichem und Auftragsverarbeiter hat der Mediator eine **Auftragsverarbeitungsvereinbarung (AVV)** gemäß Art. 28 Abs. 3 DSGVO zu schließen.

- Die Firma 8x8 Inc. mit Sitz den USA[217], die das primär zur Selbstinstallation empfohlene Open Source Tool **Jitsi Meet** auch auf eigenen Servern anbietet, hält insoweit keine AVV auf ihren Webseiten vor und bleibt im Folgenden daher, ebenso wie die auf öffentlichen Instanzen ohne AVV-Angebot nicht gewerblich betriebenen Dienste auf der Basis von Jitsi[218], außer Betracht.
- Gleiches gilt für den empfohlenen Videokonferenzdienst **BigBlueButton** der Fa. BigBlueButton Inc.[219] mit Sitz in Kanada. Ihm liegt ebenfalls quelloffene Software zugrunde, er ist primär zur Selbstinstallation vorgesehen. Die öffentlich betriebenen Instanzen sind zahlreich[220], bieten aber keine AVV.

Im Zuge der Vereinbarung der Auftragsverarbeitung ist zu beachten, dass das Datenschutzrecht bei zu Mediationszwecken organisierten Videokonferenzen, ausgehend von den personenbezogenen Daten der Parteien in zweierlei Hinsicht greift[221]:

Zum einen schließen die Parteien direkt mit dem Anbieter der Konferenzdienste einen Nutzungsvertrag, der sie dazu berechtigt, über die Infrastruktur an der vom Mediator organisierten Videokonferenz teilzunehmen. Zum anderen vereinbaren die Parteien mit dem Mediator die Durchführung der Videokonferenz zum Zwecke

---

[215] GDD Praxishilfe DS-GVO XVI 4-2020, S. 8.
[216] So Simitis/Hornung/Spiecker-*Petri* Art. 28 Rn. 30ff. m. w. N. zum Streitstand.
[217] https://www.8x8.com/.
[218] Siehe die Liste bei Digitalcourage Blog 28.04.2020.
[219] https://bigbluebutton.org/.
[220] Siehe die Liste bei Digitalcourage Blog 28.04.2020.
[221] Das zugrundeliegende Dreieck der vertraglichen Beziehungen ist oben in Abschnitt 5.2 bereits dargestellt worden.

der Mediation, und dieser schließt wiederum mit dem Anbieter einen Vertrag, der ihm die Organisation erlaubt.

Es muss daher in der Praxis wie folgt nach den verschiedenen **Datenarten** differenziert werden:

Für alle Daten, die der Dienstanbieter direkt bei den Parteien erhebt und dann verarbeitet, ist primär der Dienstanbieter als Verantwortlicher gegenüber den Parteien in ihrer Rolle als Betroffene anzusehen. Je nach Gestaltung des Videokonferenzangebotes umfasst dies in Bezug auf den der Nutzung zugrundeliegenden Dauervertrag u. U. Folgendes[222]:

- die zur Einrichtung und zum Bestehen des Nutzerkontos erforderlichen Daten, deren Erhebung und Verarbeitung gem. Art. 6 Abs. 1 lit. b DSGVO legitimiert ist (z. B. angegebener Name, Email-Adresse, ggf. Telefonnummer, Geburtsdatum);
- die beim Download und bei der Nutzung der Anwendung erhobenen und verarbeiteten Daten, die hierzu ebenfalls gem. Art. 6 Abs. 1 lit. b DSGVO notwendig sind (z. B. Informationen über das vom Nutzer verwendete Gerät, Betriebssystem und den eingesetzten Browser);
- ggf. weitere personenbezogene Daten, zu deren Erhebung und Verarbeitung der jeweilige Nutzer gemäß den Nutzungsbedingungen und Datenschutzregelungen direkt gegenüber dem Anbieter gem. Art. 6 Abs. 1 lit. a DSGVO seine Einwilligung gibt (z. B. die Nutzung der Email-Adresse für Werbezwecke, oder für das passgenaue Anbieten „interessanter Werbung"); und
- ggf. weitere personenbezogene Daten, deren Erhebung und Verarbeitung über berechtigte Interessen gem. Art. 6 Abs. 1 lit. f DSGVO legitimiert werden, wie bspw. Standortinformationen (Ort des nächstgelegenen Einwahlknotens), die der Anbieter für seine zukünftige Kapazitätsplanung verwendet.

Für alle Daten, die dagegen bei der konkreten Nutzung der Videokonferenz anfallen und verarbeitet werden, ist nun zu beachten, dass der Mediator im Einzelfall die Videokonferenz aufsetzt, den Parteien die Teilnahme ermöglicht und schließlich die Konferenz selbst als Moderator leitet. Er agiert als Veranlasser dieses Ereignisses, hat einen größeren Einfluss auf dessen Gestaltung und damit eine weiterreichende

---

[222] Siehe die Beispiele für Zoom unter https://zoom.us/privacy und für Google Meet die Beispiele unter https://policies.google.com/privacy?hl=de.

Rolle als die nur teilnehmenden Parteien. Seine Rolle als Verantwortlicher gegenüber den Teilnehmern als Betroffenen bezieht sich damit auf diejenigen Daten, deren Erhebung und Verarbeitung konkret für die Durchführung der Videokonferenz im Einzelfall erfolgen[223]. Für diese Datenverarbeitungen ist der Videokonferenz-Anbieter dann sein Auftragsverarbeiter. Dazu zählen insbes. die folgenden Daten:

- personenbezogene **Metadaten** der Kommunikation, d. h. bspw. die IP-Adresse der Endgeräte, von dem aus die Teilnehmer den Link aufrufen, der Videokonferenz beitreten und an ihr teilnehmen, sowie Zeitpunkt und Dauer der zwischen diesen IP-Adressen bestehenden Konferenz; und
- personenbezogene **Inhaltsdaten,** die im Rahmen der Videokonferenz anfallen, d. h. Audio- und Videoinhalte der Kommunikation, sowie ggf. per Screen-Sharing geteilte Inhalte und bspw. der Chatverlauf.

Schließlich ist eine Verarbeitung personenbezogener Daten durch den Anbieter der Videokonferenz, die über das unmittelbar für die Vertragserfüllung Erforderliche hinausgeht, keine Auftragsverarbeitung. Insoweit ist der Anbieter als Verantwortlicher gegenüber den Betroffenen anzusehen[224].

Diese Verarbeitung kann über Art. 6 Abs. 1 lit. f DSGVO legitimiert sein, wenn **berechtigte Interessen** gegenüber den Interessen der Betroffenen überwiegen. Dies ist bspw. der Fall bei der Erstellung und Verwendung konferenzbezogener Logdateien, die dem Anbieter helfen, Fehler zu finden, um damit die Konferenzleistungen sicherer und besser zu machen. Insoweit handelt der Anbieter nicht im Auftrag des Mediators als Konferenz-Organisator sondern im eigenen Interesse. Gleiches gilt für weitere Verarbeitungen für Anbieter-eigene Zwecke, für die der Anbieter gem. Art. 6 Abs. 1 lit. a DSGVO die Einwilligung der Betroffenen einholen möchte. Als Verantwortlicher sollte der Anbieter dies zweckmäßigerweise direkt mit allen Teilnehmern der Videokonferenz vereinbaren. Entsprechende Regelungen finden sich i. d. R. in dem Privacy-Statement des Anbieters, das den Teilnehmern angezeigt und durch die Nutzung oder durch Click akzeptiert wird[225].

Sind derartige Verarbeitungen für Anbieter-eigene Zwecke dagegen (auch) in der AVV aufgeführt, hat gemäß der Abgrenzung in Art. 28 Abs. 10 DSGVO der

---

[223] So differenzierend GDD Praxishilfe DS-GVO XVI 4-2020, S. 8.

[224] So bereits im Jahre 2010 zu Hosting-Dienstanbietern im Internet die Art. 29-DSG, WP 169, S. 31. Aktuell LfD Nds FAQ VK 8-2020, S. 5 u. EDSA Leitlinien 07/2020, S. 25.

[225] Siehe bspw. https://alfaview.com/de/privacy/, II ff.; https://sichere-videokonferenz.de/datenschutz/, 1f.; https://wire.com/de/legal/#privacy, 3ff.; sehr strukturiert und ausführlich https://zoom.us/de-de/privacy.html#_Toc44414842.

Anbieter den Mediator als Vertragspartner hierauf in der AVV ausdrücklich hinzuweisen und durch den Abschluss der AVV zunächst dessen Zustimmung einzuholen. Im Verhältnis zwischen dem Mediator und den Parteien ist dann eine Legitimation über deren **Einwilligung** als Betroffene für die Zwecke des Dienstanbieters einzuholen. Der Mediator muss die Parteien also seinerseits über diese Verarbeitungen informieren und die Parteien müssen ihre Einwilligung erteilen. Dies ist für den Mediator riskant, da er insoweit für die vollumfängliche Informiertheit der Betroffenen ebenso wie für die Freiwilligkeit deren Einwilligung für fremde Zwecke Sorge tragen muss.

Die konkrete AVV muss die Arten der verarbeiteten Daten, die Betroffenen, sowie die Verarbeitungen und Zwecke beschreiben[226] und darüber hinaus insbes. den **inhaltlichen Vorgaben des Art. 28 Abs. 3 DSGVO** genügen[227]. Sie hat neben der grundsätzlichen Weisungsgebundenheit des Auftragsverarbeiters (lit. a)[228] und der Pflicht zur Vertraulichkeitswahrung (lit. b)[229] auch Lösch- bzw. Rückgabepflichten nach Abschluss der Verarbeitung im Rahmen der Videokonferenz (lit. g)[230], den Einsatz geeigneter technischer und organisatorischer Maßnahmen (lit. c i. V. m.

---

[226] Siehe bspw. aus den in **Anhang 4** aufgelisteten Vereinbarungen alfaview AVV § 1; Microsoft DPA S. 6f. u. S. 8 (leider nicht nummeriert und nicht spezifisch für Videokonferenzen, daher auch nicht spezifisch in Bezug auf Datenarten); sichere-videokonferenz.de AVV Ziff. 2 u. 3; Wire AVV Ziff. 1.2-1.4; Zoom DPA Ziff. 3.2 i. V. m. Exhibit A.

[227] Dies wird gerade in Bezug auf Microsoft in Europa sehr unterschiedlich bewertet: Während Österreich im Oktober 2020 eine großangelegte Digitalisierungsinitiative zusammen mit Microsoft gestartet hat (siehe https://www.sn.at/wirtschaft/oesterreich/microsoft-baut-cloud-rechenzentrum-in-oe-um-1-milliarde-euro-94464037) ist die Bewertung des EDSB an dieser Stelle durchaus kritisch (siehe EDSB Microsoft Public Paper 02.07.2020 und EDSB Strategy Schrems II 30.10.2020). Die von der DSK durchgeführte und nur mit knapper Mehrheit angenommene Bewertung der Microsoft Vertragsbedingungen setzte leider auf einem inzwischen veralteten Stand auf (siehe LDA Bayern, LfDI BW PM 02.10.2020).

[228] alfaview AVV §§ 4 (1) u. 6; Microsoft DPA Anl. 3, Ziff. 2. (a); sichere-videokonferenz.de AVV Ziff. 4 (1) u. 10; Wire AVV Ziff. 1.7; Zoom DPA Ziff. 3.2 (Überraschenderweise umfasst die durch das DPA erteilte Anfangsweisung gem. Zif. 3.2 S. 2 auch die weisungsfremde Verarbeitung durch Zoom aufgrund geltenden Rechts, das entgegen Art. 28 Abs. 3 lit. a DSGVO nicht nur das Recht der EU oder ihrer Mitgliedstaaten umfasst, sondern jegliches Recht, dem Zoom als Anbieter unterliegt. Zu diesem Problem sogleich in 7.5.2 und den folgenden Abschnitten.

[229] alfaview AVV § 4 (6); Microsoft DPA S. 11; sichere-videokonferenz.de AVV Ziff. 4 (3)–(5); Wire AVV Ziff. 3.2; Zoom DPA Ziff. 4.

[230] alfaview AVV § 10; nur in Bezug auf die Vertragsbeendigung in Microsoft DPA S. 11 u. Anh. 3 Ziff. 2 g); sichere-videokonferenz.de AVV Ziff. 6, 11; Wire Ziff. 7.1; Zoom DPA Ziff. 3.4.

Art. 32)[231], sowie umfangreiche Unterstützungspflichten und Auditrechte (litt. e und h)[232] zu enthalten. Der Einsatz von Unterauftragsverarbeitern (Abs. 2 und 4) ist nur im Rahmen einer Zustimmungs- oder Einspruchslösung zulässig, i. d. R. werden die eingesetzten Unterauftragsverarbeiter in Anhängen aufgelistet[233]. Die Tätigkeit des Dienstanbieters ist damit „eine datenverarbeitende Hilfsfunktion" im Lager des Mediators als dem Verantwortlichen[234]. Dieser bleibt für die Rechtsmäßigkeit der Verarbeitung zwar vollständig haftbar, jedoch besteht daneben die Haftung des Auftragsverarbeiters gem. Art. 82 Abs. 2 S. 2 DSGVO, soweit er seine vertraglichen oder gesetzlichen Datenschutzpflichten verletzt. Die AVV muss gem. Art. 28 Abs. 9 DSGVO schriftlich oder in elektronischem Format geschlossen werden, was die Anwendungsfälle der §§ 126 a und 126 b BGB umfasst[235].

7.4.3. Weitere Fragen

Zum Teil wird pauschal der Einsatz von **Open Source Lösungen** empfohlen[236]. Der Vorteil der quelloffenen Software wird damit begründet, dass offenes Coding bestmögliche Transparenz biete und insbesondere nicht verdeckte Optionen zu unerwünschtem Speichern oder Ausleiten von Daten enthielte[237]. Dagegen führen Anbieter proprietärer Software ins Feld, dass sie anspruchsvollen Qualitätssicherungsmechanismen unterliegen und im Falle einer erkannten Sicherheitslücke dafür einstehen, diese schnellstmöglich im Rahmen des Produktsupports zu schließen[238]. Eine abschließende Beurteilung ist im Rahmen der vorliegenden Arbeit nicht möglich.

---

[231] alfaview AVV § 3 i. V. m. Anlage 1; Microsoft DPA S. 8f. i. V. m. Anh. A und Anh. 3 Ziff. 2 (c) und 4; sehr generisch in sichere-videokonferenz.de AVV Ziff. 5 (1); Wire Ziff. 4 i. V. m. Webseite; sehr ausführlich in Zoom DPA Ziff. 6 i. V. m. Exhibit B.

[232] alfaview AVV § 4 (4) u. (7), §§ 7f.; Microsoft DPA S. 8, 10, sowie Anh. 3 Ziff. 2 (e) u. (f); sichere-videokonferenz.de AVV Ziff. 4 (6)–(7), Ziff. 8 (4) u. (5); Wire AVV Ziff. 2.2, 3.1 u. 3.3; Zoom DPA Ziff. 9.

[233] alfaview AVV § 9 i. V. m. Anlage 2; Microsoft DPA S. 11f.; sichere-videokonferenz.de AVV Ziff. 7 i. V. m. Anlage 1; Wire AVV Ziff. 6; Zoom DPA Ziff. 5 mit Verweis auf Webseite.

[234] John/Wellmann DuD 2020, 506, 509.

[235] Simitis/Hornung/Spiecker-*Petri* Art. 28 Rn. 92.

[236] LfD Nds FAQ VK 8-2020, S. 12; ausdrücklich nicht mehr als Empfehlung in BBDI Hinweise VK 18.02.2020, bspw. für Jitsi Meet auf S. 14 aber noch in BBDI Checkliste VK 03.07.2020, S. 1.

[237] BBDI Empfehlungen VK 03.07.2020, S. 3f.

[238] Siehe beispielsweise die Beschreibung der „Sicherheitswartung" für Microsoft Produkte unter https://www.microsoft.com/de-de/msrc/windows-security-servicing-criteria?rtc=1.

Und schließlich stellt sich die Frage nach dem **Verarbeitungsort**. Gem. Art. 1 Abs. 3 DSGVO besteht zur Ermöglichung des freien und unbeschränkten Datenverkehrs ein harmonisiertes Datenschutzniveau innerhalb des EWR[239]. Manche Anbieter haben daher entsprechend der einhelligen Empfehlung der in den Stellungnahmen der Datenschutzbehörden[240] ihre Verarbeitungen explizit auf die EU bzw. den EWR beschränkt[241].

Dies führt zum nächsten Thema: Unter welchen Voraussetzungen ist der Export der personenbezogenen Daten in Drittstaaten bzw. ihre Verarbeitung außerhalb des EWR datenschutzrechtlich zulässig?

7.5. Internationale Anbieter und Übermittlung in Drittländer

Gerade große internationale Dienstanbieter (wie Microsoft Teams, GoogleMeet und Zoom) verwenden zum Hosting des Videokonferenzdienstes eigene Server in den USA. In diesen Fällen finden offensichtlich Übermittlungen personenbezogener Daten (Audio-, Videoinhalte, Chatverläufe) in Drittländer gem. Art. 44 S. 1 DSGVO statt.

Aber auch schon dann, wenn zwar die Server zum Betrieb des Videokonferenzdienstes im EWR stehen, so dass an sich die personenbezogenen Daten den geografischen Bereich nicht verlassen, jedoch durch IT-Aministrationstätigkeiten aus den USA heraus die Möglichkeit des Drittlandszugriffs[242] oder ihrer Kenntnisnahme von außerhalb des EWR[243] besteht, weil bspw. im EWR ein Rechenzentrum eines US-amerikanischen Konzerns genutzt wird[244], sind insoweit die Regeln der Artt. 44 ff. DSGVO zu beachten[245].

---

[239] Die Ausdehnung des Wortlauts erfolgte über die Aufnahme der DSGVO in Art. 7 lit. a EWR-Abkommen zum 20.07.2018.

[240] GDD Praxishilfe DS-GVO XVI 4-2020, S. 4.; BBDI Empfehlungen VK 03.07.2020, S. 3f.; LfD Nds FAQ VK 8-2020, S. 7.; LfDI BW PM 17.04.2020.

[241] So alfaview AVV § 1 (6) u. sichere-videokonferenz.de AVV 4 (10), nicht bei Wire AVV 1.6.

[242] Ehmann/Selmayr-*Zerdick* Art. 44 Rn. 7.

[243] Simitis/Hornung/Spiecker-*Schantz* Art. 44 Rn. 10.

[244] Siehe bspw. den Hinweis auf Amazon Web Services (AWS) bei Wire AVV, 6.1.

[245] Grages CR-online.de Blog 12.11.2020 mit Hinweis auf EDSA Empfehlungen 01/2020, Rn. 13.

Ein **Drittlandstransfer** i. S. d. Art. 44 S. 1 DSGVO ist in diesen Fällen durch die Übermittlung bzw. bereits durch die Möglichkeit des Zugriffs auf zwischengespeicherte personenbezogene Konferenzdaten gegeben. Er ist gemäß dem auch hier geltenden Verbotsprinzip nur zulässig, soweit er durch einen der in Kapitel V DSGVO beschriebenen Mechanismen umfasst wird[246]. Hintergrund dieser Regelung ist das grundrechtlich geschützte Interesse der Betroffenen an einem gleichwertigen Schutzniveau für ihre personenbezogenen Daten, unabhängig vom Ort der Verarbeitung[247].

7.5.1. Art. 45 Abs. 3 DSGVO Angemessenheitsbeschluss

Für manche Länder, wie bspw. Israel, Japan, Neuseeland und die Schweiz, besteht bereits ein sog. Angemessenheitsbeschluss der EU, der diesen Ländern ein der DSGVO entsprechendes Datenschutzniveau bestätigt[248]. Dies führt dazu, dass für Datenexporte dorthin keine besonderen Regelungen erforderlich sind[249]. Dies kann bspw. für den Transfer an den Schweizer Anbieter Wire herangezogen werden.

7.5.2. Art. 45 Abs. 1 DSGVO und das EU Datenschutzschild

Für diejenigen Dienstanbieter, die ihren Sitz jedoch in den USA und/oder sind aufgrund ihrer Konzernstrukturen darauf angewiesen sind, eine Verarbeitung auch in den USA durchzuführen, ist Folgendes zu beachten.

In den USA besteht – insbesondere aufgrund des föderalen Systems aber auch wegen der grundsätzlich eher zurückhaltenden staatlichen Regulierung in Bezug auf private Rechtsverhältnisse – eine sehr heterogene Datenschutzlandschaft[250].

Überdies gibt es keine zentrale Datenschutzaufsichtsbehörde und auch verfassungsrechtlich keine dem Recht auf informationelle Selbstbestimmung vergleichbare Verankerung des Datenschutzes[251]. Und schließlich wird vertreten, dass nur

---

[246] Simitis/Hornung/Spiecker-*Schantz* Art. 44 Rn. 9.

[247] Simitis/Hornung/Spiecker-*Schantz* Art. 44 Rn. 6.

[248] https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.

[249] So z. B. im ersten Schritt für die Beauftragung des in der Schweiz ansässigen Dienstanbieters Wire, siehe Wire AVV; dort allerdings nicht vollständig eingehalten wegen der Beauftragung von AWS, die Drittlands-verarbeitung einschließt.

[250] Simitis/Hornung/Spiecker-*Schantz* Art. 44 Rn. 42.

[251] Simitis/Hornung/Spiecker-*Schantz* Art. 44 Rn. 42.

Personen, die dauerhaft in den USA leben oder US-Staatsbürger sind, überhaupt in den Schutzbereich der in den USA geltenden vereinzelten Privacy-Regelungen einbezogen seien[252], und damit eben nicht Immigranten, aber eben bspw. auch nicht Bürger der Mitgliedsstaaten des EWR.

Vor diesem Hintergrund wurde zwischen der EU und den USA am 12. Juli 2016 auf der Grundlage des EU DSS-Beschlusses das sogenannte „EU Datenschutzschild", oder auch „**Privacy Shield-**Abkommen", verabschiedet, das am 01. August 2016 in Kraft trat. Es löste seinen Vorgänger, den „**Safe Harbor**-Pakt" ab, der bereits durch das EuGH Urteil v. 06.10.2015, „Schrems", C-362/14, EU:C:2015:650[253] für ungültig erklärt worden war. Privacy Shield enthielt u. a. detaillierte Regelungen zum Schutz der Rechte der Betroffenen gegen Eingriffe in den USA, sowie Rechtsschutzmechanismen im Falle der Verletzung. Es erlaubte den freien Transfer personenbezogener Daten an Unternehmen, die in den USA eine entsprechende Selbstzertifizierung durchgeführt hatten und galt insoweit als Angemessenheitsbeschluss gem. Art. 45 Abs. 1 DSGVO[254].

Auch die Wirksamkeit des durch Privacy Shield vermittelten Schutzes wurde jedoch bezweifelt und die Gültigkeit schließlich ebenfalls vom EuGH in seinem Urteil vom 16.07.2020, „**Schrems II**", C-311/18, EU:C:2020:559 verneint[255]. Entgegen der noch im EU DSS-Beschluss vertretenen Einschätzung, dass ein Zugriff auf personenbezogene Daten insbesondere im Kontext geheimdienstlicher Tätigkeit aus Gründen der nationalen Sicherheit in den USA (auch wenn kein richterlicher Einzelfall-Beschluss erforderlich sei[256]) auf das Notwendigste beschränkt sei und damit im Einklang mit geltendem EU Datenschutzrecht stehe[257], kam der EuGH in

---

[252] Siehe die Hinweise bei Simitis/Hornung/Spiecker-*Schantz* Art. 44 Rn. 43 und den Executive Order 13768 des US Präsidenten Trump vom 25.01.2017, durch den die Anwendung sämtlicher Gesetze zum Schutz der Privatsphäre oder personenbezogener Daten aus Gründen der nationalen Sicherheit auf US-Bürger oder -Einwohner eingeschränkt wird (siehe https://trumpwhitehouse.archives.gov/presidential-actions/executive-order-enhancing-public-safety-interior-united-states/). Dieser EO 13768 ist allerdings inzwischen durch US Präsident Joe Biden am 21.01.2021 aufgehoben worden, siehe unter https://www.whitehouse.gov/briefing-room/presidential-actions/2021/01/20/executive-order-the-revision-of-civil-immigration-enforcement-policies-and-priorities/, dort Section 2.

[253] Abrufbar über die Suchmaske des EuGH unter https://curia.europa.eu/jcms/jcms/j_6/de/; Maximilian Schrems ist ein österreichischer Jurist und Datenschutzaktivist, siehe https://noyb.eu/de/unser-team-mitglieder-und-partner.

[254] Simitis/Hornung/Spiecker-*Schantz* Art. 45 Rn. 47.

[255] Abrufbar über die Suchmaske des EuGH unter https://curia.europa.eu/jcms/jcms/j_6/de/.

[256] EG 109 zum EU DSS-Beschluss.

[257] EG 140 zum EU DSS-Beschluss.

Schrems II nun insbesondere wegen der Möglichkeit der sicherheitsbehördlichen Anordnung einer flächendeckenden Kommunikationsüberwachung zu der gegenteiligen Auffassung[258]. Auch der Rechtsschutz gegen derartige Eingriffe sei in den USA weder durch Gerichte noch durch die Privacy Shield Ombudsperson (mangels deren Unabhängigkeit von der Exekutive) ausreichend gegeben[259]. Infolgedessen erklärt der EuGH den EU DSS-Beschluss in Gänze für unwirksam[260].

Somit stellt das Privacy Shield seit dem 17.07.2020 nicht nur zwischen den Parteien des zugrundeliegenden Rechtsstreits sondern allgemeingültig[261] keine Rechtsgrundlage für die Übermittlung personenbezogener Daten in die USA mehr dar[262]. Eine Übergangsfrist wurde durch den EuGH nicht gewährt[263]. Allerdings wurden die Arbeiten zum Entwurf eines neuen Übereinkommens, das an die Stelle von Privacy Shield treten soll, zwischen der EU und den USA bereits am 10. August 2020 aufgenommen[264] und inzwischen „intensiviert“[265].

7.5.3. Art. 46 Abs. 2 lit. c DSGVO und EU SDK

Als alternatives Rechtsinstrument kommen die **EU Standarddatenschutzklauseln** (EU SDK), ehemals „Standardvertragsklauseln“ genannt, in Betracht[266].

Sie wurden zwar von der EU noch auf Basis der Datenschutz-RL beschlossen, boten jedoch auch i. S. d. Art. 46 Abs. 2 lit. c DSGVO grundsätzlich geeignete Garantien für den Fall der Übermittlung personenbezogener Daten von einem im EWR

---

[258] EuGH Urteil – C-311/18, Rn. 184.
[259] EuGH Urteil – C-311/18 Rn. 197.
[260] EuGH Urteil – C-311/18 Rn. 201.
[261] LfDI BW OH VK 07.09.2020, S. 5.
[262] Es findet sich allerdings in der Form einer Selbstverpflichtung noch in den AVVen einiger Anbieter, siehe Microsoft DPA S. 11; dagegen unklar bei Zoom DPA Ziff. 7.
[263] EuGH Urteil – C-311/18 Rn. 202.
[264] Siehe die gemeinsame Presseerklärung der EU Kommission und des US DOC, gemäß Presseerklärung der EU Kommission unter https://ec.europa.eu/info/news/joint-press-statement-european-commissioner-justice-didier-reynders-and-us-secretary-commerce-wilbur-ross-7-august-2020-2020-aug-07_en
[265] Siehe die Pressemeldung der EU Kommission unter https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_21_1443.
[266] Eine Einbeziehung der SDK als maßgebliche Legitimation für Datenexporte findet sich z. B. in Microsoft DPA S. 10 i. V. m. Anl. 2 und in Zoom DPA Ziff. 7, wo nach der Neufassung im Dezember 2020 nun nicht mehr SDK und Datenschutzschild alternativ nebeneinander als Rechtsgrundlagen angeführt werden.

ansässigen Verantwortlichen an Auftragsverarbeiter in Drittländern ohne angemessenes Datenschutzniveau[267]. Sie sind zur Vereinbarung zwischen diesen beiden Parteien gedacht und beinhalten detaillierte Regelungen insbes. mit dem Ziel zu gewährleisten, dass die Datenverarbeitung auch im Drittland im Einklang mit der DSGVO erfolgt und die Rechte und Grundfreiheiten der Betroffenen angemessen geschützt werden. Ihre Verletzung führt u. a. zu einem Klagerecht der Betroffenen[268].

Bislang wurde ihre Vereinbarung als wirksames Rechtsinstitut für den Drittlandstransfer angesehen, seit dem EuGH Urteil Schrems II reichen sie jedoch nicht mehr aus. Insbesondere da allein die Vereinbarung vertraglicher Regelungen nicht dazu geeignet sei, im Drittland den Zugriff von Behörden auf die transferierten personenbezogenen Daten einzuschränken[269], habe der Verantwortliche – ggf. zusammen mit dem im Drittland ansässigen Auftragsverarbeiter – für das jeweilige Drittland zu prüfen, ob über die EU SDK hinaus **weitere Garantien zum Schutz der Rechte der Betroffenen und ihrer Durchsetzung** i. S. d. Art. 46 Abs. 1 DSGVO erforderlich seien[270]. Diese habe er dann zu ergreifen[271].

Die grundsätzliche Erforderlichkeit zusätzlicher Maßnahmen wurde vom EuGH für Transfers in die USA bereits bejaht. Wie bei der Prüfung des Privacy Shield stellt der EuGH auch insoweit fest, dass in den USA kein angemessenes Datenschutzniveau besteht, so dass die Verwendung der EU SDK ohne zusätzliche weitere technische, organisatorische und /oder vertragliche Garantien als Rechtsinstitut für den Transfer in die USA schlicht nicht mehr ausreicht[272].

Auch diese Vorgabe wirkt über den konkreten Rechtsstreit hinaus, da sie als Auslegungsregel von allen Datenschutzbehörden im Geltungsbereich der DSGVO zu beachten ist[273]. Sie erntete Zustimmung jedoch auch **Kritik**: In US-amerikanischen Stellungnahmen wird auf die Verunsicherung hingewiesen, die das Urteil für die Weltwirtschaft mit sich bringe, die auf den freien Datenverkehr zwischen den

---

[267] EG 8 zu den EU SDK.
[268] EG 19 zu den EU SDK.
[269] EuGH Urteil – C-311/18, Rn. 125.
[270] EuGH Urteil – C-311/18, Rn. 134.
[271] EuGH Urteil – C-311/18, Rn. 132f. unter Berufung auf EG 109 zur DSGVO.
[272] EuGH Urteil – C-311/18, Rn. 154 i. V. m. 141f. u. der ausdrückliche Hinweis in Microsoft DPA S. 11.
[273] LfDI BW OH VK 07.09.2020, S. 5f.

Kontinenten angewiesen sei[274]. Das US DOC hat überdies ein Whitepaper veröffentlicht, das den europäischen Richtern insbesondere vorwirft, sie hätten das US Recht nicht hinreichend genau geprüft[275]. Europäische Stimmen weisen auf die offenen Datenschutzfragen bei Tätigkeiten europäischer Geheimdienste hin und drängen auf eine politische Abstimmung auf internationaler Ebene[276]. Die Kritik ändert allerdings nichts an den Auswirkungen des EuGH Urteils in der Praxis.

Für die Prüfung, welche weiteren Garantien konkret erforderlich sind, und für deren Einhalten ist bei der Mediation über Videokonferenz der Mediator als Verantwortlicher zuständig und rechenschaftspflichtig. Die zur Prüfung und Umsetzung notwendigen Anforderungen hat der EDSA Anfang November 2020 in zwei ausführlichen Empfehlungen[277] in Form eines **Sechs-Schritte-Vorgehens**[278] niedergelegt:

Jeder Verantwortliche, also vorliegend der Mediator, wird darin aufgerufen, folgendes zu evaluieren[279]:

1. Kenntnis aller Übermittlungen personenbezogener Daten in Drittländer und Prüfung der Notwendigkeit;
2. Wahl des geeigneten Übermittlungsinstruments;
3. Beurteilung der Rechtslage im Drittland und Vergleich mit dem Datenschutzniveau im EWR;
4. Beurteilung der Effektivität der zusätzlichen Maßnahmen, insbes. im Zusammenhang mit der konkreten Datenübermittlung und der Rechtslage;
5. Einhaltung der ggf. erforderlichen förmlichen Verfahrensschritte, z. B. Rücksprache mit der Aufsichtsbehörde; und
6. Wachsamkeit und regelmäßige Prüfung der Veränderungen in den Drittländern.

---

[274] Siehe die Darstellung des US DOC Secretary of State unter https://www.commerce.gov/about/letter-deputy-assistant-secretary-james-sullivan-schrems-ii-decision.
[275] US DOC SCC Whitepaper, S. 6ff.
[276] Sehl LTO Blog 21.10.2020.
[277] EDSA Empfehlungen 01/2020 und EDSA Empfehlungen 02/2020.
[278] Fennessy iapp Blog 11.11.2020.
[279] Zusammenfassend eingangs der EDSA-Empfehlungen 01/2020, S. 2–4.

Zugleich hat die EU Kommission einen neuen **Entwurf der EU SDK** als Konkretisierung der vertraglichen Maßnahmen publiziert und zu öffentlichem Feedback aufgefordert[280].

Für die **Praxis** ergibt sich daraus Folgendes: Bei der Durchsicht der Empfehlungen fällt auf, dass der EDSA zwar in den praktischen Beispielen[281] durchaus im Austausch mit der Wirtschaft konkrete Anwendungsfälle berücksichtigt und durchgespielt hat[282]. Allerdings sind – begründet durch die bedingungslosen Vorgaben des EuGH Urteils Schrems II – die Anforderungen so detailliert und strikt (nach den Kritikern geradezu praxisfern[283]), dass es nicht nur einer aufwändigen Analyse durch IT- und Datenschutz-Experten[284] bedarf, sondern u. a. auch der internationalen Rechtsberatung: Nach der exakten Beschreibung der jeweiligen Datentransfers[285] und der Wahl des einschlägigen Transfermechanismus aus Kap. V der DSGVO[286] ist rechtlich zu evaluieren, welchen Risiken die personenbezogenen Daten durch die nicht adäquate Rechtsordnung des Drittstaats im Vergleich zum Schutz der Rechte und Freiheiten der Betroffenen gemäß der GRCh[287] unterliegen[288]. Diese Prüfung umfasst nicht nur die Transparenz und Präzision der Eingriffsbefugnisse gem. Art. 8 Abs. 2 GRCh[289], sondern auch die Verhältnismäßigkeit der erlaubten Eingriffe[290], die Unabhängigkeit des Aufsichtssystems[291] und den Individualrechtsschutz für die Betroffenen[292]. Schließlich sind dann geeignete Maßnahmen zur Kompensation zu definieren[293], umzusetzen[294] und regelmäßig auf ihre

---

[280] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12741-Commission-Implementing-Decision-on-standard-contractual-clauses-for-the-transfer-of-personal-data-to-third-countries.
[281] EDSA Empfehlungen 01/2020, Rn. 78ff.
[282] Grages CR-online.de Blog 12.11.2020; Fennessy iapp Blog 11.11.2020.
[283] Grages CR-online.de Blog 12.11.2020.
[284] Fennessy iapp Blog 11.11.2020.
[285] EDSA Empfehlungen 01/2020, Rn. 8ff.
[286] EDSA Empfehlungen 01/2020, Rn. 14ff.
[287] Dazu EDSA Empfehlungen 01/2020, Rn. 36 und im Detail EDSA Empfehlungen 02/2020, Rn. 24ff.
[288] EDSA Empfehlungen 01/2020, Rn. 28ff., insbes. 32f.
[289] EDSA Empfehlungen 02/2020, Rn. 26ff.
[290] EDSA Empfehlungen 02/2020, Rn. 32ff.
[291] EDSA Empfehlungen 02/2020, Rn. 39ff.
[292] EDSA Empfehlungen 02/2020, Rn. 43ff.
[293] EDSA Empfehlungen 01/2020, Rn. 45ff. i. V. m. Annex 2.
[294] EDSA Empfehlungen 01/2020, Rn. 55ff.

Wirksamkeit hin zu evaluieren[295]. Insbesondere die folgenden Bereiche organisatorischer, technischer und vertraglicher Maßnahmen werden ausführlich beleuchtet:

Die **organisatorischen Maßnahmen** umfassen bspw. regelmäßige Transparenzberichte zu behördlichen und geheimdienstlichen Auskunftsersuchen im Drittland[296]. Dies wird auch heute schon bspw. von den Anbietern der Tools Microsoft Teams[297] und GoogleMeet[298] publiziert.

Als **technische Maßnahme** wird insbesondere die **Verschlüsselung** thematisiert[299]. Dabei zwar auf europäischer Ebene nicht pauschal gefordert, dass sie nicht geheimdienstlich gebrochen werden kann[300], jedoch muss sie zertifiziert sein, dem Stand der Technik entsprechen und als „robust gegenüber möglicher behördlicher Kryptoanalyse" im Drittland anzusehen sein[301]. Es werden also nicht nur die regelmäßig vorhandene Verschlüsselung zentral gespeicherter Daten (wie ggf. Chatverläufe oder Aufzeichnungen) und eine Transportverschlüsselung im aktuellem Stand[302] gefordert, sondern generell (und nicht nur bei erhöhtem Schutzbedarf)[303] eine zuverlässige Ende-zu-Ende-Verschlüsselung. Durch sie werden die Daten nicht nur beim Transit zwischen den Teilnehmern und den Übermittlungsservern, sondern auch beim Zwischenspeichern auf diesen vor dem unbefugten Zugriff bewahrt[304], indem die Daten auf den Servern nicht entschlüsselt werden, und letztlich auch die Schlüssel nicht beim Dienstanbieter, sondern nur bei den Beteiligten liegen[305]. Backdoors dürfen nicht vorhanden sein[306]. Dies, die Aussage, dass gem. dem lokal anwendbaren Recht die Behörden keine Schlüssel herausverlangen dürfen[307],

---

[295] EDSA Empfehlungen 01/2020, Rn. 62ff.
[296] EDSA Empfehlungen 01/2020, Rn. 129.
[297] https://www.microsoft.com/en-us/corporate-responsibility/law-enforcement-requests-report.
[298] https://transparencyreport.google.com/user-data/overview, wo man in der Visualisierung den Anstieg der Anzahl an Auskunftsersuchen erkennt.
[299] EDSA Empfehlungen 01/2020, Rn. 79.
[300] So bspw. jedoch LfDI BW OH VK 07.09.2020, S. 7.
[301] EDSA Empfehlungen 01/2020, Rn. 79 u. 84.
[302] BSI Kompendium VK 4-2020, S. 67f. und 89; DSK OH VK 23.10.2020, S. 18.
[303] BSI Kompendium VK 4-2020, S. 102f.; DSK OH VK 23.10.2020, S. 19, die allerdings unterstellt, sie sei noch nicht marktgängig.
[304] BSI Kompendium VK 4-2020, S. 25.
[305] EDSA Empfehlungen 01/2020, Rn. 79 für Backup-Storage und 84 für Routing durch Drittländer.
[306] EDSA Empfehlung 01/2020, Rn. 84.
[307] EDSA Empfehlungen 01/2020, Rn. 103 mit Fn. 80.

sowie passende Informations- und Haftungsregelungen[308] sollten zusätzlich als vertragliche Maßnahme vom Dienstanbieter zugesagt werden. Während Ende-zu-Ende-Verschlüsselung Stand April 2020 noch als „in der Regel für Videokonferenzen nicht praktikabel" beschrieben wurde[309], gibt es inzwischen einige Anbieter, die hiermit werben, u. a. Zoom[310].

Diese Anforderung wird jedoch zukünftig schwierig zu erfüllen sein, da der EU Rat unter deutscher Ratspräsidentschaft am 06.11.2020 just unter der Überschrift „Security through encryption and security despite encryption" in einem zunächst nicht-öffentlichen, aber geleakten Entwurf[311] forderte zügig zu beschließen, dass die Anbieter von Ende-zu-Ende verschlüsselter Kommunikation den zuständigen Behörden, nicht nur zu Zwecken des Staatsschutzes und der nachrichtendienstlichen Tätigkeit, sondern allgemein zu Strafverfolgungszwecken den Zugriff und die Entschlüsselung ermöglichen müssen. Dieser Beschluss wurde am 14.12.2020 wirksam veröffentlicht[312]. Dies würde bedeuten, dass der Anbieter entgegen den Datenschutzforderungen über einen „Generalschlüssel" verfügen müsste, der an den eingesetzten Servern dazu verwendet werden kann, jegliche verschlüsselten Kommunikationsinhalte zu entschlüsseln und ihr Abhören zu ermöglichen[313]. Die öffentliche Hand steht der Ende-zu-Ende-Verschlüsselung von Kommunikation insgesamt kritisch gegenüber, da sie zu strafbaren Zwecken missbraucht werden kann und letztlich dem öffentlichen Sicherheitsinteresse widerspricht[314]. Die Ent-

---

[308] Siehe den Hinweis auf die Aktualisierung bei Brill Microsoft Blog 20.11.2020; äußerst kritisch allerdings Bergt CR-online.de Blog 22.11.2020.

[309] BSI Kompendium VK 4-2020, S. 103.

[310] Nach dem Streit um angebliche Ende-zu-Ende Verschlüsselung im Frühjahr 2020 (siehe Gal Zoom Blog 01.04.2020), hat Zoom dies nun zumindest für die auf einer App basierende Nutzung in der Praxis umgesetzt. Siehe dazu Zoom Whitepaper E2E Encryption.

[311] Abrufbar u. a. bei https://www.heise.de/downloads/18/2/9/9/8/5/2/0/783284_fh_st12143-re01en20_783284.pdf.

[312] Siehe die Presseerklärung des EU Rats unter https://www.consilium.europa.eu/de/press/press-releases/2020/12/14/encryption-council-adopts-resolution-on-security-through-encryption-and-security-despite-encryption/, den Beschluss unter https://data.consilium.europa.eu/doc/document/ST-13084-2020-REV-1/de/pdf und den aktuellen Überblick über die aktuelle Debatte bei don't panic TU Berlin Blog 30.04.2021.

[313] Moechel ORF 08.11.2020; Sokolov heise.de 09.11.2020; siehe auch die Zusammenstellung der Kritik bei Krempl heise.de 13.11.2020.

[314] Siehe hierzu die Stellungnahme der EU-Kommission vom 24.07.2020, S. 16, unter https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/20200724_com-2020-607-commission-communication_en.pdf.

wicklungen bleiben insoweit abzuwarten. Eine „magische Lösung", die sowohl sicher ist (im Sinne der EDSA Forderungen), als auch Zugriffe bestimmter Behörden ermöglicht, stellt – gelinde gesagt –eine Herausforderung dar[315].

Als **vertragliche Maßnahmen** werden vom EDSA insbesondere die Zusage gefordert, dass der Dienstanbieter sich gegen Herausgabeverlangen drittstaatlicher Behörden wehren und, wo möglich, den Betroffenen informieren müsse[316]. Microsoft erklärt, man habe dies – und weitergehende Pflichten – inzwischen umgesetzt[317].

Abschließend ist festzustellen, dass diese geforderte Vorgehensweise zwar auf einen lückenlosen und zuverlässigen Datenschutz ausgerichtet ist, angesichts der Komplexität des Themas und der der EDSA-Forderung, diese Maßnahmen im Einzelfall zu kombinieren, in der Praxis nicht ohne IT-Fachberatung und einschlägigen Rechtsrat, auch zu ausländischen Rechtsordnungen zu bewältigen ist[318]. Kritiker weisen darauf hin, dass selbst bei umfassender Beratung Restrisiken nicht auszuschließen sind[319].

So wie der einseitig durch die DSGVO festgelegte globale Datenschutzstandard letztlich in einen außenpolitischen Arbeitsauftrag an die EU Institutionen mündet[320], müssen die einseitig durch die Rechtsordnungen der Drittstaaten aufgestellten Regelungen und die Datenschutzforderungen der EU durch internationale Übereinkommen zukünftig aneinander angepasst werden. Stattdessen bürdet der EDSA durch die Empfehlungen den Anwendern derzeit auf, diese durch die Globalisierung der Wirtschaft entstandenen Disparitäten nationaler oder regionaler Rechtsordnungen im Alltag zu lösen[321]. Diese Forderungen sind durch die Anwender nicht, jedenfalls nicht kurzfristig, zu erfüllen.[322]

Nur als „Ironie am Rande" [323] sei erwähnt, dass sich Betroffene gem. der Ausnahme in Art. 2 Abs. 2 lit. d DSGVO[324] in Europa zwar über die JI-RL (und in

[315] Siehe zuletzt Ermert heise.de 20.11.2020.
[316] EDSA Empfehlungen 01/2020, Rn. 112f. u. 118f.
[317] Brill Microsoft Blog 20.11.2020; kritisch allerdings Bergt CR-online.de Blog 22.11.2020 m. w. N..
[318] So auch CEP Studie, S. 42.
[319] Grager CR-online.de Blog 12.11.2020.
[320] Simitis/Hornung/Spiecker-*Schantz* Art. 44 Rn. 7f.
[321] Grager CR-online.de Blog 12.11.2020.
[322] So auch CEP Studie, S. 15.
[323] Härting beck-aktuell 24.08.2020.
[324] Siehe auch EG 16 zur DSGVO.

Deutschland über die Umsetzung in §§ 45ff. BDSG) gegenüber Strafverfolgungsbehörden, aber nicht gegenüber europäischen Geheimdiensten auf den Schutz der DSGVO bzw. die GRCh berufen können[325].

7.5.4. Art. 49 DSGVO und Ausnahmen für bestimmte Fälle

Für die Erlaubnis des Transfers ist schließlich noch zu prüfen, ob einer der Ausnahmetatbestände des Art. 49 DSGVO in Betracht kommt[326]. Sie greifen nur subsidiär in Fällen, in denen andere Rechtsinstitute wie die eben beschriebenen aus Artt. 45f DSGVO nicht gegeben sind. Sie sind überdies eng auszulegen, damit durch sie nicht das allgemeine Schutzniveau der DSGVO unterlaufen wird[327].

Art. 49 Abs. 1 UA 1 lit. b DSGVO legitimiert in Anlehnung an Art. 6 Abs. 1 lit. b DSGVO Transfers zur **Vertragserfüllung**, jedoch beschränkt auf gelegentliche Fälle[328]. Eine Nutzung von US-Servern für die Durchführung von Videokonferenzen ist auf dieser Grundlage wegen der damit einhergehenden dauerhaften und wiederholten Transfers nicht möglich. Auch eine Anwendung auf Fälle, in denen die Server im EWR stehen und nur gelegentlich durch Administration oder Fernwartungszugriffe die Möglichkeit des Kontakts mit personenbezogenen Daten bestehen kann, scheidet aus, da zwischen diesen Tätigkeiten und der Erbringung der eigentlichen Konferenzleistung kein unmittelbarer Zusammenhang[329] besteht. Auch eine Begründung, dass die mit der Nutzung weit verbreiteter und bequem nutzbarer Videokonferenzlösungen einhergehende Verwendung US-amerikanischer Infrastruktur schlicht dienlich sei, scheitert an dem Erforderlichkeitskriterium[330].

Art. 49 Abs. 1 UA 1 lit. a DSGVO erlaubt schließlich eine Übermittlung soweit eine wirksame ausdrückliche **Einwilligung** der Betroffenen erteilt worden ist. Diese Regelung honoriert die Privatautonomie der Parteien im Interesse ihrer informationellen Selbstbestimmung. Sie dürfen darüber entscheiden, wie viel Schutz sie für ihre personenbezogenen Daten wünschen. Die DSGVO „drängt den Schutz nicht

---

[325] Brauneck EuZW 2020, 933, 937.
[326] So explizit der abschließende Hinweis im EuGH Urteil Schrems II – C-311/18, Rn. 202.
[327] EDSA Leitlinien 02/2018, S. 3f.
[328] EG 111 zur DSGVO; bei Auslandsbezug auch erweiternd EDSA Leitlinien 02/2018, S. 10.
[329] Simitis/Hornung/Spiecker-*Schantz* Art. 49 Rn. 21.
[330] Siehe der Hinweis bei Simitis/Hornung/Spiecker-*Schantz* Art. 49 Rn. 22.

auf‘[331], sondern ist im Kern freiheitswahrend. Das Ausmaß der gewünschten Freiheit ist dabei Sache des Einzelnen. Kann nun eine Einwilligung insoweit die Übermittlungen in ein nicht-sicheres Drittland legitimieren?

Die wirksame Einwilligung der Parteien setzt eine informierte und freiwillige Entscheidung voraus, für die neben den allgemeinen Kriterien (Zweck der Übermittlung, Art von Daten, Recht zum Widerruf der Einwilligung, Identität oder Kategorien der Empfänger) insbesondere auch die Beschreibung des Risikos erforderlich ist, dem der Betroffene in Bezug auf seine Daten aufgrund des nicht angemessenen Schutzniveaus im Drittland und aufgrund der fehlenden angemessenen Garantien ausgesetzt ist[332]. Es muss also eine ausreichende Risikoaufklärung stattfinden.

Hier bietet sich ein Vergleich zur Diskussion über den Verzicht auf Verschlüsselung bei **Emails im Verkehr zwischen Rechtsanwälten und ihren Mandanten** an. Allgemein wird datenschutzrechtlich für Emails, die personenbezogene Daten enthalten, zumindest eine Transportverschlüsselung auf der Basis von TLS im aktuellen Stand gefordert. Nur bei Emails, bei denen ein Bruch der Vertraulichkeit von personenbezogenen Daten im Inhalt der Nachricht ein hohes Risiko für die Rechte und Freiheiten von natürlichen Personen darstelle, sei dagegen darüber hinaus eine Ende-zu-Ende-Verschlüsselung notwendig[333]. Es wird darauf hingewiesen, dass selbst die Email-Kommunikation über das besondere Anwaltspostfach (beA), dessen Nutzung in mehreren Stufen bis 2022 für Rechtsanwälte verpflichtend wird, keine Ende-zu-Ende-Verschlüsselung im engeren Sinne aufweise, da die zur Entschlüsselung notwendigen Keydaten auf dem zentralen Server lägen, und nicht ausschließlich bei Sender und Empfänger[334].

Bei Einwilligung des Betroffenen werden unverschlüsselte Emails daher als zulässig angesehen[335]. Diese Einwilligungserklärung kann ausdrücklich oder auch konkludent[336] durch das eigene Eröffnen unverschlüsselter Email-Kommunikation

[331] Kremer ITRB 2020, 35, 38.
[332] EDSA Leitlinien 02/2018, S. 9.
[333] DSK PM E-Mail 26.05.2020.
[334] Keppeler CR 2019, 18, 19 m. w. N.
[335] Bertolino ZKM 2019, 60, 68 m. w. N.
[336] Auer-Reinsdorff/Conrad-*Lapp* § 30 Rn. 33.

seitens des Mandanten erfolgen. Der Rechtsanwalt oder Mediator ist nur aufgerufen, den Betroffenen über einen allgemeingehaltenen Hinweis ohne technische Einzelheiten über das damit verbundene Risiko aufzuklären[337].

Diese knappe Form der Information reicht wohl für Videokonferenzen mit US Berührung angesichts der EDSA Empfehlungen nicht mehr aus: Im Fall der Videokonferenz müsste der Mediator die Parteien darüber aufklären, welche Daten wo im Detail verarbeitet werden, dass der Dienstanbieter (oder der Betreiber der von ihm eingesetzten Server im EWR) dem geltenden US-Recht unterliegt, aus dem sich erweiterte behördliche Zugriffsbefugnisse ergeben, und erläutern, dass – wie in den EDSA Empfehlungen 2/2020 beschrieben – keine vergleichbaren Datenverarbeitungsregeln bestehen und kein gleichwertiger Rechtsschutz gegeben ist[338]. Darüber hinaus müsste die Aufklärung die ergriffenen Abhilfemaßnahmen beschreiben. Dies ist – wie eben in Abschnitt 7.5.3 gezeigt – in der Praxis ohne ausführliche Analyse durch IT- und Rechtsexperten nicht zu bewältigen.

Außerdem wird durch die ausdrückliche Anordnung eines rein objektiven Prüfungsmaßstabs des EDSA, der zunächst und vor allem auf die Rechtslage im Drittland abstellt[339], der ansonsten im Datenschutzrecht (siehe bspw. Art. 24 Abs. 1 DSGVO) geltende Grundsatz der interessengerechten Risikobetrachtung nach Schwere des möglichen Schadens und Eintrittswahrscheinlichkeit[340] überschrieben. Eine dem Interesse der Privatautonomie der Parteien entsprechende Abwägungsentscheidung für Videokonferenztools, die um den Vorteil besserer Übertragungsqualität, Stabilität und Funktionshaltigkeit ggf. weniger Datenschutz und Sicherheit bieten[341], ist damit nicht mehr möglich.

Und schließlich war die Ausnahmevorschrift des Art. 49 Abs. 1 UA 1 lit. a DSGVO, anders als lit. b und e im selben Unterabsatz, nach dem Willen des Verordnungsgebers[342] nicht auf gelegentliche Übermittlungen beschränkt und daher auch für Legitimation wiederkehrender Transfers geeignet. Auch dieser e-contrario Auslegung hat der EDSA allerdings eine Absage erteilt[343]. D. h. selbst bei Erfüllung

---

[337] Kremer ITRB 2020, 35, 40.

[338] Siehe auch bereits die EDSA Leitlinien 02/2018, S. 9f.

[339] EDSA Empfehlungen 01/2020, Rn. 42.

[340] DSK Kurzpapier Nr.18., S. 2ff, insbes. S. 4f.; zu Emails auch Kremer ITRB 2020, 35, 38.

[341] So der Vorschlag von Kilburg Komet Blog 14.07.2020.

[342] EG 111 zur DSGVO.

[343] EDSA Empfehlungen, 01/2020 Rn. 25.

aller Voraussetzungen für eine wirksame Einwilligung ist diese Vorschrift nicht als Grundlage für über das Internet stattfindende, regelmäßige internationale Verarbeitungen geeignet.

7.5.5. Exkurs zum CLOUD Act

Auch wenn sich das EuGH Urteil Schrems II in seinen Ausführungen auf nationales US-Sicherheitsrecht und Geheimdienstbefugnisse beschränkt, gibt es außerhalb dessen überdies allgemein das Problem der Geltung lokalen Rechts[344], das mit EU Datenschutzrecht in Konflikt stehen kann, insbesondere den US CLOUD Act[345]: Die Herausgabe personenbezogener Daten, die bei einem Service Provider anfallen und verarbeitet werden (also vorliegend insbesondere die Metadaten aber auch die Inhalte der Videokommunikation) ist sowohl gem. Art. 6 Abs. 1 lit. c DSGVO (Erfüllung einer rechtlichen Verpflichtung) als auch gem. Art. 6 Abs. 1 lit. e DSGVO (Notwendigkeit im öffentlichen Interesse) wegen Art. 6 Abs. 3 DSGVO nur zulässig, wenn das Herausgabeverlangen (als Form der Verarbeitung) auf geltendes EU Recht oder das Recht eines Mitgliedsstaates gestützt wird[346]. Eine entsprechende explizite Verpflichtung des Auftragsverarbeiters enthält überdies Art. 28 Abs. 3 lit. a DSGVO. Das Recht von Drittländern darf gem. Artt. 48 sowie 49 UA 1 lit. d u. Abs. 4 DSGVO nur dann als Grundlage für eine durch drittstaatliche Behörden oder Gerichte angeordnete Herausgabe von personenbezogenen Daten herangezogen werden, wenn dies über eine internationale Übereinkunft, insbesondere also ein Rechtshilfeabkommen zwischen dem Drittland und der EU oder dem Mitgliedsstaat, vorgesehen ist[347]. Es gibt durchaus entsprechende Verträge zwischen der EU bzw. Deutschland und den USA[348]. Der **US CLOUD Act** wurde jedoch durch die USA gezielt als effizientes Rechtsinstrument neben langwierige Rechtshilfeverfahren gestellt[349]. Er erstreckt ein in den USA beschlossenes behördliches oder gerichtliches Herausgabeersuchen über in den USA gehostete Server hinaus auf solche Server, die – gleich in welcher geografischen Lokation – in dem Besitz oder unter der Kontrolle (possession, custody or control) eines US-Unternehmens stehen[350].

---

[344] BSI Kompendium VK 4-2020, S. 36.

[345] John/Wellmann DuD 2020, 506, 510.

[346] EDSA Joint Response Cloud Act 10.07.2019, Annex S. 4ff., wo auch die Rechtfertigung über Art. 6 Abs. 1 lit. f DSGVO verneint wird, da dies dem Schutzzweck der DSGVO zuwiderlaufe.

[347] Simitis/Hornung/Spiecker-*Schantz* Art. 49 Rn. 36.

[348] Siehe bspw. das EU-USA Rechtshilfeabkommen.

[349] US DOJ CLOUD Act Whitepaper, S. 10f.

[350] US DOJ CLOUD Act Whitepaper, S. 15f.

D. h. das reine Hosting auf Servern in Deutschland oder in Europa durch ein US-Unternehmen oder ein im EWR ansässiges verbundenes Unternehmen eines US Konzerns schützt nicht vollständig vor der Anwendbarkeit des US Rechts.

Dies läuft regulären **Prinzipien des Völkerrechts** zuwider, die die Durchsetzung eines drittstaatlichen Herausgabeersuchens nur über bilaterale oder multilaterale Rechtshilfeabkommen erlauben. Während im Rahmen der Entscheidung über ein Rechtshilfeersuchen der ersuchte Staat das lokale Datenschutzrecht aber auch Verschwiegenheitspflichten zu beachten hat[351], bleibt unklar, welche konkreten Abwägungen ein US Gericht gemäß dem CLOUD Act im Fall des Konflikts mit Datenschutzrecht vornehmen würde[352]: Gemäß CLOUD Act Section 103 (b) ist eine Berufung des Betroffenen auf europäisches Datenschutzrecht zum Schutz vor der Herausgabe auf der Grundlage geltenden US Rechts erst dann möglich, wenn die USA mit der EU ein auf den CLOUD Act bezogenes Abkommen geschlossen haben[353]. Bis dahin sind die US Gerichte gemäß CLOUD Act Section 103 (c) nur gehalten, im Falle des Konflikts des Herausgabeersuchens mit dem Recht der EU und andere Länder ohne Abkommen anhand der schwach konturierten „Einvernehmlichkeitsgrundsätze internationalen Rechts“ (Comity Analysis) zu entscheiden. Dies stellt keinen hinreichenden Rechtsschutz im Sinne der DSGVO dar[354]. Damit ergibt sich auch außerhalb des im EuGH Urteil Schrems II thematisierten, über US-Sicherheitsgesetze drohenden Verstoßes gegen Datenschutzrecht, ein weiteres Risiko für personenbezogene Daten, die von US Konzernen auch im EWR auf ihren Servern verarbeitet werden.

7.5.6. Fazit zur internationalen Verarbeitung / zur Verarbeitung durch internationale Anbieter

Es muss daher zum Zeitpunkt der Erstellung der vorliegenden Arbeit davon ausgegangen werden, dass ein Einsatz US-amerikanischer Dienstanbieter für Videokonferenzen im Rahmen von Mediationen nicht datenschutzkonform möglich ist. Gleiches gilt für europäische Dienstanbieter, die Server verwenden, die von US-Kon-

---

[351] Siehe bspw. die Vorgaben in Art. 9 des EU-USA Rechtshilfeabkommens.

[352] US DOJ CLOUD Act Whitepaper, S. 16.

[353] Mit Großbritannien und Australien wurden entsprechende Vereinbarungen bereits getroffen, siehe die Dokumentation unter https://www.justice.gov/dag/cloudact. Die Verhandlungen mit der EU haben am 26.09.2019 begonnen, siehe das Joint US-EU Statement on Electronic Evidence Sharing Negotiations vom 26.09.2019, abrufbar unter https://www.justice.gov/opa/pr/joint-us-eu-statement-electronic-evidence-sharing-negotiations.

[354] Siehe dazu oben bereits im Kontext der Darstellung des EuGH Urteils Schrems II.

zernen im EWR gehostet aber aus den USA administriert werden: Es darf zwar berücksichtigt werden, dass hierbei nur gelegentlich im Kontext der Administration der Zugriff auf dort für Videokonferenzen zwischengespeicherte personenbezogene Daten (oder zentral gespeicherte Daten wie Chatverläufe) nicht auszuschließen ist, aber es darf eben nicht darauf basierend eine Wahrscheinlichkeitsbeurteilung fremdstaatlicher Zugriffe zur Risikoermittlung erfolgen.

Die rechtlich sicherste Lösung ist, die beschriebenen Drittlandtransfers in die USA komplett zu vermeiden, und personenbezogene Daten so im EWR zu speichern und zu verarbeiten, dass US-Unternehmen oder US-Konzerngesellschaften keine Kontrolle darüber haben. Letztlich sind daher ausschließlich europäische Dienstanbieter ohne US-Unterauftragsverarbeiter rechtssicher nutzbar.[355]

Die internationalen Dienstanbieter wie bspw. Microsoft stehen derzeit im engen Austausch mit den Datenschutzbehörden. Ein Beispiel hierfür ist der inzwischen allerdings gescheiterte[356] Pilotversuch des Einsatzes von Microsoft Produkten zu Schulzwecken in Baden-Württemberg[357]. Sie haben ihre AVVen und Verarbeitungen angepasst[358] und planen, weitere technische und/oder organisatorische Abhilfemaßnahmen ergreifen. Es bleibt abzuwarten, wie sich die EDSA-Empfehlungen in der Praxis bewähren. Die EU hat überdies im November 2020 einen Vorschlag für die Aktualisierung der EU SDK erarbeitet, zu dem der EDSA und der EDSB in der Folge eine gemeinsame Stellungnahme erarbeitet und veröffentlicht haben[359]. Weder eine Neufassung des Datenschutzschilds,[360] noch überarbeitete und verbesserte EU SDK vermögen jedoch die Rechtslage zu ändern, solange die USA ihre Regelungen zu Eingriffsbefugnissen nicht auf das einschränken, was gemäß EU-Recht zulässig wäre, und EU-Bürgern keinen ausreichenden Rechtsschutz dagegen einräumen[361]. Mehrere große deutsche Unternehmen haben überdies in zwei Schreiben – sowohl an die deutsche Bundesregierung als auch an die EU Kommission –

---

[355] Siehe auch CEP Studie, S. 43.

[356] Siehe Wilkens heise.de 07.05.2021 und oben Fußnote 206.

[357] Siehe bspw. Krempl heise.de 31.10.2020, LfDI BW PM 30.10.2020 u. LfDI BW PM 20.11.2020.

[358] Die Änderungshistorie bspw. für Microsoft ist abrufbar unter https://privacy.microsoft.com/de-DE/updates.

[359] EDSB/EDSA Joint Opinion 14.01.2021.

[360] Die EU und die USA haben am 25.03.2021 in einer gemeinsamen Pressemeldung verkündet, ihre Verhandlungen hierzu zu „intensivieren", siehe https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_21_1443.

[361] CEP Studie, S. III.

den Handlungsbedarf klar adressiert: Es braucht bis zum Inkrafttreten dieser Neuerungen eine Übergangslösung auf europäischer Ebene, da auch die europäische Wirtschaft maßgeblich auf internationale Datenverarbeitungen angewiesen ist[362].

Das Risiko drittstaatlicher Behördenzugriffe beim Einsatz von Videokonferenzanbietern insbesondere aus den USA wird de lege ferenda durch die geplante Anwendung des Telekommunikationsrechts (siehe Abschnitt 7.3) ebenfalls nicht gelöst. Nach US-amerikanischem Recht sind im Bereich der Telekommunikation weder Verbindungsdaten noch Inhaltsdaten in einer Weise geschützt, die sich mit dem Fernmeldegeheimnis vergleichen ließe[363]. Es bleibt daher offen, wie die entsprechenden Anbieter auf die geplante Gesetzesänderung reagieren, denn hierdurch wird der Konflikt der beiden Rechtsordnungen noch deutlicher.

7.6. Datenschutz bei der Durchführung der Videokonferenz

Setzt der Mediator nun einen rein im EWR datenverarbeitenden Videokonferenzdienst[364] ein, muss er auch bei der Durchführung der Videokonferenz geltendes Datenschutzrecht beachten.

Grundlage der Verarbeitung ist gem. Art. 6 Abs. 1 lit. b DSGVO im ersten Schritt die Erforderlichkeit zur Erfüllung des Vertrages mit der betroffenen Person bzw. zur Durchführung vorvertraglicher Maßnahmen auf Anfrage der betroffenen Person, also zur vereinbarungsgemäßen Durchführung der Mediation mittels Videokonferenz. Eine Einwilligung gem. Art. 6 Abs. 1 lit. a DSGVO sollte darüber hinaus nur für Verarbeitungsvorgänge eingeholt werden, die nicht auf dieser Grundlage legitimiert sind[365].

Im Anwendungsbereich der DSGVO hat der Mediator bei der Verarbeitung die in Art. 5 Abs. 1 DSGVO geregelten Datenverarbeitungsgrundsätze zu beachten. Hierauf ist im Folgenden einzugehen, allerdings aus systematischen Gründen nicht entsprechend der Regelungsreihenfolge der Vorschrift:

Die gebotene **Datenminimierung** Art. 5 Abs. 1 lit a DSGVO schreibt vor, dass nur solche Daten verarbeitet werden dürfen, die für die Vertragserfüllung notwendig sind. Im Kontext der Videokonferenz bedeutet dies nun Folgendes:

---

[362] Neuerer handelsblatt.de 03.05.2021 und ders. handelsblatt.de 08.05.2021.

[363] Simitis/Hornung/Spiecker-*Schantz* Art. 45 Rn. 43 m. w. N.

[364] Wie bspw. sichere-videokonferenz.de.

[365] Siehe auch Dendorfer-Ditges/Schmidt-Gorbach KD 2018, 318, 320 und zum Mandatsvertrag des Rechtsanwalts Auer-Reinsdorff/Conrad-*Lapp* § 30 Rn. 11. Ein anderer Ansatz findet sich bei Weigel Inkovema Blog 17.02.2020: Er stellt vorrangig auf die Einwilligung ab.

Die technische Verarbeitung der personenbezogenen Sprach- und Videodaten einschließlich des Zwischenspeicherns auf den zur Übermittlung eingesetzten Servern des Dienstanbieters ist für das Funktionieren der vereinbarten Videokonferenz erforderlich und daher zulässig. Darüber hinaus sollte für den Zweck der Durchführung der Mediation – wie aus Gründen der mediationsrechtlichen Vertraulichkeit – aufgrund der in Art. 5 Abs. 1 lit e DSGVO vorgeschriebenen Speicherbegrenzung die Aufzeichnung der Videokonferenz[366] in der Regel ausgeschaltet sein, es sei denn, sie wird von den Parteien ausdrücklich gewünscht, vom Mediator ebenfalls gebilligt und im Mediationsvertrag zwischen den Beteiligten im Detail unter Angabe von den damit verfolgten Zwecken, der anschließenden Speicherdauer und der einvernehmlich zulässigen Verwendung vereinbart. Unter den gleichen Grundsätzen sollten Chat-Verläufe oder Ergebnisse aus Umfragen („Polling“) nach Gesprächsende gelöscht werden[367], es sei denn, es ist auf Parteiwunsch Abweichendes vereinbart.

Außerdem ist ratsam, eventuell eingerichtete Datenübertragungen an den Anbieter auszuschalten, die in dessen Interesse eingerichtet sind, um Nutzungsstatistiken oder nicht zwingend zur Fehlerbeseitigung erforderliche Logfiles[368] oder Absturzberichte zu erhalten[369], oder sogar Aufzeichnungen für Qualitätssicherungszwecke anzufertigen[370]. In diesem Kontext wird darauf hingewiesen, dass die Nutzung der Videokonferenz über Webtools im Browser und nicht über heruntergeladene Anwendungen beim Teilnehmer in der Regel datensparsamer sei[371].

Nicht nur aus Gründen der Ressourcensparsamkeit, sondern vor allem zur Wahrung der auch datenschutzrechtlich geschützten Privatsphäre der Betroffenen wird mitunter dazu geraten, die aktive Videoübertragung auszuschalten, oder zumindest die Beteiligten auf diese Möglichkeit hinzuweisen[372]. Dies ist nachvollziehbar. Es ist im Kontext von Mediationen, für die explizit die Videokonferenz gewählt wurde, allerdings nicht dauerhaft sinnvoll. Eine Mediation via Videokonferenz ist nur unter

---

[366] Siehe auch LfD BW PM 17.04.2020.
[367] GDD Praxishilfe DS-GVO XVI 4-2020, S. 7.
[368] BSI Kompendium VK 4-2020, S. 51.
[369] LfDI BW PM 17.04.2020; GDD Praxishilfe DS-GVO XVI 4-2020, S. 7.
[370] BBDI Empfehlungen VK 03.07.2020, S. 2.
[371] LfDI BW PM 17.04.2020.
[372] LfDI BW PM 17.04.2020.

der Voraussetzung durchzuführen, dass alle Beteiligten grundsätzlich damit einverstanden sind, dass sie als Person auf den Bildschirmen der anderen Teilnehmer sichtbar sind. Gerade dies schafft die gewünschte Kommunikationsreichhaltigkeit[373] in beiden Richtungen. Es spricht nichts dagegen, vorübergehend den Ton und die Videoübertragung auszuschalten, bspw. wenn die Beteiligten eine Pause wünschen, oder bei zuvor vereinbarter Anwesenheit von Beratern, mit denen sich eine Partei vertraulich abstimmen möchte. Für den Schutz der Privatsphäre gibt es andere Maßnahmen: Der Mediator kann die Parteien auf eine geschickte Wahl des Standortes hinweisen, der keine Rückschlüsse über private Gegebenheiten zulässt[374]. Ist im eingesetzten Tool keine „Blurring"-Funktion, durch die der Hintergrund unscharf erscheint[375], oder das Einblenden eines virtuellen Hintergrunds[376] möglich, sollten die Medianden darauf hingewiesen werden, dass sie hinter sich einen Sichtschutz (Paravent) aufstellen oder sich vor einer neutralen Wand in einem Raum positionieren können[377].

Der Grundsatz der **Zweckbindung** in Art. 5 Abs. 1 lit. b DSGVO[378] bedeutet im Kern, dass eine Verarbeitung der personenbezogenen Daten nur zu dem vereinbarten Zweck erfolgen darf. Nur in diesem Umfang ist der Eingriff in das Recht auf informationelle Selbstbestimmung der betroffenen Person legitim[379]. Dieser Zweck muss hinreichend bestimmt sein. Eine Weiterverwendung für andere Zwecke verbietet sich. Dies bedeutet, dass der Mediator die für die Vertragsanbahnung und -erfüllung erhobenen personenbezogenen Daten der Parteien z. B. nicht später für Werbezwecke verwenden darf. Ist eine Werbungstätigkeit gewünscht, kann sie nur mit Einwilligung der Betroffenen[380] gemäß Art. 6 Abs. 1 lit. a DSGVO erfolgen.

Am Rande sei bemerkt, dass Mediator gemäß dem Grundsatz der **Datenrichtigkeit** in Art. 5 Abs. 1 lit. d DSGVO verpflichtet ist, die Daten zu korrigieren, wenn er Fehler erkennt, oder ein Betroffener den Berichtigungsanspruch gemäß Art. 16 Abs. 1 DSGVO geltend macht. Dieser Anspruch ist sogar als Grundrecht in Art. 8

---

[373] S. o. Abschnitt 2.3.
[374] BSI Kompendium VK 4-2020, S. 95.
[375] BSI Kompendium VK 4-2020, S. 95; BMEV Knigge VK, S. 1
[376] Siehe GDD Praxishilfe DS-GVO XVI 4-2020, S. 7.
[377] DSK OH VK 23.10.2020, S. 11f.; BMEV Knigge VK, S. 1.
[378] Auch bereits in Art. 8 Abs. 2 S. 1 GRCh.
[379] Simitis/Hornung/Spiecker-*Roßnagel* Art. 5 Rn. 65.
[380] Simitis/Hornung/Spiecker-*Schantz* Art. 6 Rn. 31.

Abs. 2 S. 2 GRCh geschützt. Allerdings wird er Parteien im Mediationsverfahren nicht über den Umweg des Datenschutzrechts dazu verhelfen, bei unterschiedlicher Auffassung oder Wertungen vom Mediator „Berichtigung" in Chatinhalten oder Aufzeichnungen verlangen zu dürfen[381].

Und schließlich beinhaltet das Datenschutzrecht den Grundsatz der **Integrität und Vertraulichkeit** in Art. 5 Abs. 1 lit. f DSGVO. Er verpflichtet den Mediator auch datenschutzrechtlich dazu, die bereits oben beschriebenen vertraulichkeitswahrenden Maßnahmen in Bezug auf personenbezogene Daten zu ergreifen, d. h. im Kontext der Videokonferenz übermittelte Audio- und Videodaten insbesondere vor dem unbefugten Zugriff Dritter zu schützen, sowie dafür zu sorgen, dass die von ihm aufbewahrten Daten nicht absichtlich oder versehentlich gelöscht oder beschädigt werden[382].

Dazu und insgesamt zur Sicherheit und Rechtmäßigkeit hat der Mediator als Verantwortlicher geeignete und angemessene **technische und/oder organisatorische Maßnahmen** gem. Artt. 24, 25, 32 DSGVO zu ergreifen[383], sowie im Detail entsprechende Pflichten in der AVV mit dem Auftragsverarbeiter zu vereinbaren. Dem Mediator obliegt es insoweit, bspw. in seinem Verantwortungsbereich die Mitarbeiter entsprechend zu schulen und zu sensibilisieren, der Schwerpunkt der zu ergreifenden Maßnahmen obliegt im Fall der Videokonferenz allerdings dem Dienstanbieter.

7.7. Weitere Datenschutzpflichten

Und schließlich treffen den Mediator als Verantwortlichen beim Einsatz von Videokonferenzen zur Mediation weitere datenschutzrechtliche Pflichten[384]:

Der Mediator hat die Durchführung der Videokonferenz zum Zweck der Mediation mit den Parteien in dem Mediationsvertrag zu vereinbaren. Auf diesem Wege kann er bspw. **Informationspflichten** aus Art. 13 DSGVO gegenüber den Medianden als Betroffenen erfüllen. Die erforderlichen Informationen sind im Detail in

[381] Siehe den Hinweis bei Auer-Reinsdorff/Conrad-*Lapp* § 30 Rn. 17.
[382] Siehe EG 39 zur DSGVO.
[383] John/Wellmann DuD 2020, 606, 609.
[384] Siehe allgemein John/Wellmann DuD 2020, 506, 509ff.

Art. 13 Abs. 1 und Abs. 2 DSGVO aufgelistet, und umfassen insbesondere die Kategorien der Daten, die Empfänger (also auch den Dienstanbieter als Auftragsverarbeiter), Grundlage und Zwecke der Verarbeitung, internationale Transfers, Verarbeitungen für eigene Zwecke des Anbieters sowie den Hinweis auf die Betroffenen-Rechte. Die Informationen müssen für einen durchschnittlichen Leser ohne übermäßigen Aufwand verständlich und transparent sein (Artt. 12 u. Art. 5 Abs. 1 lit. a DSGVO)[385]. Ein Beispiel, das (angepasst auf den Einzelfall) als Vorlage für diese Datenschutzinformation dienen kann, findet sich in **Anhang 3.**

Eine Information derjenigen Personen, die zwar nicht Mediand sind, über die jedoch im Rahmen der Konflikterhellung ggf. unter Einschluss personenbezogener Daten wie Name, Alter und Beziehung zu den Medianden oder zum Konfliktgeschehen während der Videokonferenz gesprochen wird, oder deren personenbezogene Daten Gegenstand von Aufzeichnungen werden, ist grundsätzlich gem. Art. 14 DSGVO erforderlich. Fraglich ist, ob sich der Mediator insoweit wegen seiner gesetzlichen Verschwiegenheitspflicht auf die Ausnahme des Art. 14 Abs. 5 lit. d DSGVO berufen darf. Der Anwendungsbereich dieser Vorschrift wird in der Literatur mitunter durch einen Hinweis auf § 203 StGB definiert[386]. Hiernach wären nur Mediatoren mit einem in § 203 Abs. 1 StGB aufgelisteten Grundberuf erfasst, deren Mediatorentätigkeit überdies zu ihrer beruflichen Tätigkeit gerechnet wird[387], so insbesondere bei Anwaltsmediatoren. Auch eine Erfassung dieser Mediatoren über § 203 Abs. 3 StGB scheidet aus, da sie bei eigener Tätigkeit auch in eigener Verantwortung handeln und – auch bei Co-Mediation – nicht nur als Hilfsperson eines anwaltlichen Mediators anzusehen sind. Da jedoch weder Art. 14 Abs. 5 DSGVO noch der einschlägige Erwägungsgrund eine Hinweis auf die Erforderlichkeit strafrechtlicher Sanktionierung der Verschwiegenheitspflicht enthalten, und neben den Berufsträgern auch satzungsmäßig zur Verschwiegenheit Verpflichtete umfasst, ist der Anwendungsbereich so zu interpretieren, dass er zumindest gesetzliche Verschwiegenheitspflichten umfasst[388]. Dadurch, dass dem Mediator insoweit eine gesetzliche, wenngleich nicht strafrechtlich abgesicherte, Verschwiegenheitspflicht obliegt, darf gem. Art. 14 Abs. 5 lit. d DSGVO eine Information dieser Betroffenen, die nicht Medianden sind, unterbleiben.

Darüber hinaus darf jeder Betroffene unter den Voraussetzungen des Art. 17 Abs. 1 DSGVO ein Recht auf **Löschung** geltend machen. Bspw. steuerrechtliche

---

[385] DSK OH VK 23.10.2020, S. 13f.
[386] Simitis/Hornung/Spiecker-*Dix* Art. 14 Rn. 30 m. w. N.
[387] Haft/Schlieffen-*Eisele* § 46 Rn. 14; Lackner/Kühl-*Heger* § 203 Rn. 16.
[388] BeckOK DatenschutzR-*Schmidt-Wudy* DSGVO Art. 14 Rn. 105f.

Aufbewahrungspflichten, denen der Mediator unterliegt, gehen der Löschungspflicht gemäß Art. 6 Abs. 1 lit. c und Art. 17 Abs. 1 i. V. m. Abs. 3 lit. b DSGVO vor, soweit hierfür die erhobenen Daten erforderlich sind. Dies umfasst wohl Vertrags- und Abrechnungsdaten, aber beispielsweise nicht die elektronische Dokumentation der Gespräche oder von den Parteien elektronisch überlassene Dokumente.

Sofern ohnehin – insbes. aufgrund umfangreichen IT-Einsatzes in größeren Mediationsbüros oder Anwaltskanzleien – ein **Verarbeitungsverzeichnis** gem. Art. 30 DSGVO geführt wird, ist das Durchführen von Videokonferenzen dort aufzunehmen[389].

Im Falle von „Datenpannen" hat der Mediator gem. Art. 33 DSGVO **Meldepflichten** gegenüber den Aufsichtsbehörden und **Benachrichtigungspflichten** Art. 34 DSGVO gegenüber den Betroffenen. Die AVV enthält hierzu entsprechende Informations- und Unterstützungspflichten des jeweiligen Dienstanbieters[390].

Der Mediator als Verantwortlicher hat gemäß dem Vorstehenden bei seiner risikobasierten Entscheidung über Auswahl und Betriebsdetails des Videokonferenzdienstes bereits die Interessen und Rechte der Betroffenen angemessen berücksichtigt[391]. Eine Pflicht zur Durchführung einer **Datenschutz-Folgenabschätzung** gemäß Art. 35 DSGVO ist mangels umfangreicher Verarbeitung besonderer Datenkategorien im Rahmen der videokonferenzgestützten Mediation daher zu verneinen.

Allerdings trifft den Mediator gemäß dem Gebot der Transparenz und der Rechenschaft nach Art. 5 Abs. 2 DSGVO die Pflicht zur **Dokumentation** der Einhaltung der Datenschutzgrundsätze bei Auswahl und Einsatz des Dienstes**,** um die Prüfung der Aufsichtsbehörden zu ermöglichen[392].

I. d. R. wird für Mediatoren keine Pflicht zur **Bestellung eines Datenschutzbeauftragten** (DSB) bestehen. Zum einen liegt gem. Art. 37 Abs. 1 DSGVO die Haupttätigkeit der Mediatoren – anders als bspw. bei Arztpraxen[393] – nicht in der umfangreichen Verarbeitung besonderer Datenkategorien i. S. d. Art. 9 DSGVO o-

[389] DSK OH VK 23.10.2020, S. 16.
[390] Siehe z. B. alfaview AVV § 4 (7); sichere-videokonferenz.de AVV, 9; Wire AVV, 5; Zoom DPA, 9.5f.
[391] Siehe auch John/Wellmann DuD 2020, 606, 608.
[392] LfD Nds FAQ VK 8-2020, S. 5f.
[393] So Art. 29-DSG, WP 243 rev. 01, S. 8f.

der auch personenbezogener Daten im Kontext des Strafrechts oder Strafprozessrechts gemäß Art. 10 DSGVO[394]. Zum anderen liegen auch die Voraussetzungen des § 38 BDSG i. V. m. der Öffnungsklausel in Art. 37 Abs. 4 S. 1 Hs. 2 DSGVO nicht vor, nach denen ein DSB in jedem Fall zu bestellen ist, wo regelmäßig eine Mindestanzahl von zwanzig[395] (in der Vorversion des BDSG: zehn[396]) Personen ständig mit der automatisierten (also IT-gestützten) Verarbeitung personenbezogener Daten betraut ist.

[394] Dies übersieht Weigel Inkovema Blog 17.02.2020.

[395] BGBl. 2019 Teil I S. 1634, Art. 12 Änderung des Bundesdatenschutzgesetzes, Ziff. 9.

[396] BGBl. 2017 Teil I S. 2097, Art. 1 Änderung des Bundesdatenschutzgesetzes, S. 2113, und hierauf Bezug nehmend wohl Auer-Reinsdorff/Conrad-*Lapp,* § 30 Rn. 4.

8. Fazit und Empfehlungen für die Praxis

Der zunehmende Einsatz von Videokonferenzen für Zwecke der Mediation eröffnet Parteien und Mediatoren einen niederschwelligen Zugang zu dieser Form der Streitbeilegung. Er wirft allerdings besondere Fragestellungen im Kontext der Vertraulichkeit und des Datenschutzrechts sowohl bei der Auswahl und Beauftragung eines geeigneten Konferenzdienstes als auch bei der Durchführung der Mediation auf.

Grundlegend sind hier die Interessen der Parteien am Schutz ihrer Privatsphäre und ggf. auch ihrer Geschäftsgeheimnisse, sowie an der Bewahrung der konstruktiven Atmosphäre der Mediation zu beachten. Parallel ist aber auch das Bedürfnis wichtig, vor der Gefahr unkontrollierter Verwendung der personenbezogenen Daten geschützt zu werden.

Der Mediator, der den Einsatz von Videokonferenzdiensten zur Mediation erwägt, hat daher (ggf. zusammen mit den Parteien) einen geeigneten Dienst, insbesondere anhand der Vertraulichkeits- und Datenschutzanforderungen, auszuwählen und auch während der Durchführung der Videokonferenz mithilfe von wählbaren Einstellungen des Produktes sowie durch Vereinbarungen mit den Parteien dafür Sorge zu tragen, dass die Vertraulichkeit eingehalten wird.

Nach dem derzeitigen Stand sowohl der europarechtlichen Vorgaben als auch der verfügbaren Funktionen der Dienstangebote kommen für einen datenschutzrechtlich sicheren Einsatz nur Videokonferenzdienste von Anbietern ohne Verbindungen zu US-Konzernen in Betracht, bei denen überdies die Verarbeitung personenbezogener Daten auf den EWR und/oder solche Staaten beschränkt ist, für die ein Angemessenheitsbeschluss der EU vorliegt.

Ein Einsatz international verarbeitender Anbieter kann nur nach einer eingehenden IT-Sicherheits- und Datenschutzprüfung anhand des jeweils aktuellen Stands der Sicherheitsfunktionen des Videokonferenzdienstes, der jeweiligen Vertragsbedingungen und der Rechtslage am Ort der Verarbeitung empfohlen werden. Gängige Videokonferenztools US-amerikanischer Anbieter sind im Zweifel derzeit nicht rechtssicher nutzbar.

Auf europäischer und internationaler Ebene werden politische und rechtsetzende Anstrengungen zur Lösung dieses Problems unternommen. Gleichzeitig entwickeln Dienstanbieter technische Neuerungen zur Datensicherheit und aktualisieren ihre vertraglichen Zusagen in enger Abstimmung mit den Datenschutzbehörden.

Es bleibt daher abzuwarten, wie sich die Rechtslage in Bezug auf Drittlandsverarbeitungen, insbesondere in den USA oder durch US-amerikanische Anbieter in europäischen Rechenzentren entwickelt. Wünschenswert wäre eine transatlantische

Abstimmung in Bezug auf behördliche und/oder geheimdienstliche Eingriffsbefugnisse in Abwägung zu geltendem Datenschutzrecht, einschließlich einer einheitlichen Sicht auf die Zulässigkeit wirksamer Verschlüsselungsmechanismen.

Literaturverzeichnis

Art. 29-DSG, WP 169: Artikel-29-Datenschutzgruppe, WP169 – 00264/10/DE – Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher“ und „Auftragsverarbeiter“, angenommen am 16. Februar 2016, deutsche Sprachfassung abrufbar auf den Seiten des BfDI: https://www.bfdi.bund.de/SharedDocs/Publikationen/Dokumente-Art29Gruppe_EDSA/Stellungnahmen/WP169_Opinion12010ConceptsControllerProcessor.html.

Art. 29-DSG, WP 243 rev. 01: Artikel-29-Datenschutzgruppe, WP 243 rev. 01 – 16/DE – Leitlinien in Bezug auf Datenschutzbeauftragte („DSB“), angenommen am 13. Dezember 2016, zuletzt überarbeitet und angenommen am 5. April 2017, bestätigt vom EDSA unter https://edpb.europa.eu/node/69, deutsche Sprachfassung abrufbar auf den Seiten des BfDI: https://www.bfdi.bund.de/SharedDocs/Publikationen/Dokumente-Art29Gruppe_EDSA/Guidelines/WP243_DPO_DE.html.

Auer-Reinsdorff/Conrad-*Bearbeiter*: Astrid Auer-Reinsdorff, Isabell Conrad, Handbuch IT- und Datenschutzrecht, 3. Auflage 2019.

BBDI Checkliste VK 03.07.2020: Berliner Beauftragte für Datenschutz und Informationsfreiheit, Checkliste für die Durchführung von Videokonferenzen während der Kontaktbeschränkungen, Version 1.4 vom 03.07.2020, abrufbar unter https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/orientierungshilfen/2020-BlnBDI-Checkliste_Videokonferenzen.pdf.

BBDI Empfehlungen VK 03.07.2020: Berliner Beauftragte für Datenschutz und Informationssicherheit, Orientierungshilfe Berliner Datenschutzbeauftragte zur Durchführung von Videokonferenzen während der Kontaktbeschränkungen, 03.07.2020, abrufbar unter https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/orientierungshilfen/2020-BlnBDI-Empfehlungen_Videokonferenzsysteme.pdf.

BBDI Hinweise VK 18.02.2021: Berliner Beauftragte für Datenschutz und Informationssicherheit, Hinweise für Berliner Verantwortliche zu Anbietern von Videokonferenzdiensten Version 2.0, 18.02.2021, abrufbar unter https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/orientierungshilfen/2021-BlnBDI-Hinweise_Berliner_Verantwortliche_zu_Anbietern_Videokonferenz-Dienste.pdf.

BeckOK-DatenschutzR-*Bearbeiter*: Stefan Brink, Heinrich Amadeus Wolff (Hrsg.), BeckOK Datenschutzrecht, 33. Edition, Stand 01.08.2020.

Beck TKG-*Bearbeiter*: Martin Geppert, Raimund Schütz (Hrsg.), Beck'scher TKG-Kommentar, 4. Auflage 2013.

Bergt CR-online.de Blog 22.11.2020: Matthias Bergt, Zusatz zu Standardvertragsklauseln: Massenweise Nebelkerzen von Microsoft und manchen Datenschutz-Aufsichtsbehörden, 22.11.2020, abrufbar unter https://www.cr-online.de/blog/2020/11/22/zusatz-zu-standardvertragsklauseln-massenweise-nebelkerzen-von-microsoft-und-manchen-datenschutz-aufsichtsbehoerden/.

Bertolino ZKM 2019, 58: Camilla Bertolino, Datenschutz im Mediationsbüro, in ZKM 2019, S. 58-62.

BMEV Knigge VK: Bundesverband Mediation e.V., Knigge für Videokonferenzen Empfehlung des Vorstands des Bundesverband MEDIATION e.V., kein Datum, abrufbar unter https://www.bmev.de/fileadmin/downloads/oeffentlichkeitsarbeit/Videokonferenz-Knigge_Empfehlung_BM.pdf.

BRAK Hinweise VK: Bundesrechtsanwaltskammer, Hinweise zum Thema Videokonferenzen – Anbieterempfehlungen, Übersichten, Links, 07.01.2021, abrufbar unter https://brak.de/fuer-anwaelte/datenschutz/videokonferenzen/.

Brauneck EuZW 2020, 933: Jens Brauneck, Privacy Shield – zu Recht für ungültig erklärt? Zugleich Besprechung von EuGH, Urt. v. 16.7.2020 in der Rs. C-311/18 – Schrems II, in EuZW 2020, S. 933–941.

Briegleb heise.de 27.10.2020: Volker Briegleb, Regierungsstreit über Vertragslaufzeiten verzögert TKV-Novelle, 27.10.2020, abrufbar unter https://www.heise.de/news/Regierungsstreit-ueber-Vertragslaufzeiten-verzoegert-TKG-Novelle-4940728.html.

Brill Microsoft Blog 20.11.2020: Julie Brill, Neue Maßnahmen zum Schutz Ihrer Daten, 20.11.2020, abrufbar unter https://news.microsoft.com/de-de/neue-massnahmen-zum-schutz-von-daten/.

BSI Kompendium VK 4-2020: Bundesamt für Sicherheit in der Informationstechnik, BSI Kompendium Videonkonferenzsysteme, KoViKo – Version 1.0.1, April 2020, abrufbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Kompendium-Videokonferenzsysteme.pdf;jsessionid=E289584FB2D4BB9FE2EB6AD85BDAB269.2_cid503?__blob=publicationFile&v=4.

CEP Studie: Anja Hoffmann, Unzulässigkeit der Datenübermittlung in die USA. Das EuGH-Urteil „Schrems II" und seine Folgen, Studie des Centrums für Europäische Politik, 26.01.2021, abrufbar unter https://www.cep.eu/eu-themen/details/cep/unzulaessigkeit-der-datenuebermittlung-in-die-usa-cepstudie.html.

DAV Stellungnahme MediationsG (2010): Deutscher Anwaltvererein, Stellungnahme Nr. 58/10 zum Referentenentwurf des Bundesministeriums der Justiz. Gesetz zur Förderung der Mediation und anderer Verfahren der außergerichtlichen Konfliktbeilegung (Mediationsgesetz), Aktenzeichen: R A 7 – 9340/17-2-R4 554/2010, abrufbar über die Webseite des DAV unter https://anwaltverein.de/de/.

DAV-Stellungnahme TKG (2013): Deutscher Anwaltverein (Ausschuss Informationsrecht), Stellungnahme Nr. SN 55/2013 zur Anwendung des TKG auf neue Kommunikationsplattformen (bspw. WhatsApp), abrufbar über die Webseite des DAV unter https://anwaltverein.de/de/.

Dendorfer-Ditges/Schmidt-Gorbach, KD 2018, 318: Renate Dendorfer-Ditges, Wolfgang Schmidt-Gorbach, Datenschutz 2018. Neuerungen und Herausforderungen für Mediatorinnen und Mediatoren, in KD 2018, S. 318–325.

Digitalcourage Blog 28.04.2020: Blog-Eintrag auf digitalcourage.de, Videokonferenzen müssen keine Datenschleudern sein, Stand 28.04.2020, abrufbar unter https://digitalcourage.de/digitale-selbstverteidigung/videokonferenzen-muessen-keine-datenschleudern-sein.

DIHK Alternativen zu Videokonferenz 30.03.2020: Deutscher Industrie und Handelskammertag e. V., Mögliche Alternativen zu Videokonferenz, Stand 30.03.2020, abrufbar auch über die Empfehlungs- und Informationsseiten des BMEV unter https://www.bmev.de/fileadmin/downloads/oeffentlichkeitsarbeit/DIHK_2020-03-30_Mo__gliche_Alternativen_fu__r_Softwareeinsatz_DSGVO.pdf.

don't panic TU Berlin Blog 30.04.2021: don't panic, Pseudonym eines Mitarbeiters des Team Datenschutz der TU Berlin, Crypto Wars – der Kampf um Verschlüsselung, 30.04.2021, abrufbar unter https://blogs.tu-berlin.de/datenschutz_notizen/2021/04/30/crypto-wars-der-kampf-um-verschluesselung/.

DRB Stellungnahme MediationsG (2010): Oliver Sporré, Stellungnahme des Deutschen Richterbundes zum Referentenentwurf eines Gesetzes zur Förderung der Mediation und anderer Verfahren der außergerichtlichen Konfliktbeilegung, September 2010, abrufbar unter https://www.drb.de/fileadmin/DRB/pdf/Stellungnahmen/2010/DRB_100929_Stn_Nr_35_MediationG.pdf.

DSK Kurzpapier Nr. 18: Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder, Kurzpapier Nr. 18, Risiko für die Rechte und Freiheiten natürlicher Personen, Stand 26.04.2018, abrufbar unter https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_18.pdf.

DSK OH VK 23.10.2020: Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder, Stand 23.10.2020, abrufbar unter https://www.datenschutzkonferenz-online.de/media/oh/20201023_oh_videokonferenzsysteme.pdf.

DSK PM E-Mail 26.05.2020: Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder, Schutz personenbezogener Daten bei der Übermittlung per E-Mail. Pressemitteilung, 26.05.2020, abrufbar unter https://www.datenschutzkonferenz-online.de/media/pm/20200526_pm_orientierungshilfe_uebermittlung_pbd_per_e_mail.pdf.

Duve/Eidenmüller/Hacke: Christian Duve, Horst Eidenmüller, Andreas Hacke, Mediation in der Wirtschaft. Wege zum professionellen Konfliktmanagement, 2. Auflage 2011.

EDSA Joint Response Cloud Act 10.07.2019: European Data Protection Board, European Data Protection Supervisor, EDPB-EDPS Joint Response on the US Cloud Act. EDPB-EDPS Joint Response to the LIBE Committee on the impact of the US Cloud Act on the European legal framework for personal data protection, 10.07.2019, abrufbar unter https://edps.europa.eu/data-protection/our-work/publications/opinions/edpb-edps-joint-response-us-cloud-act_en.

EDSA Empfehlungen 01/2020: European Data Protection Board, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, 10.11.2020, abrufbar unter https://edpb.europa.eu/sites/edpb/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_en.pdf.
Auf Deutsch (aber noch ohne Übersetzungsprüfung): Der Europäische Datenschutzausschuss, Empfehlungen 01/2020 zu Maßnahmen zur Ergänzung von Übermittlungstools zur Gewährleistung des unionsrechtlichen Schutzniveaus für personenbezogene Daten, 10.11.2020, abrufbar im Rahmen der öffentlichen Konsultation unter: https://edpb.europa.eu/our-work-tools/documents/public-consultations/2020/recommendations-012020-measures-supplement_de.

EDSA Empfehlungen 02/2020: Der Europäische Datenschutzausschuss, Empfehlungen 02/2020 zu den wesentlichen europäischen Garantien in Bezug auf Überwachungsmaßnahmen, 10.11.2020, abrufbar unter https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-022020-european-essential-guarantees_de.

EDSA Leitlinien 07/2020: European Data Protection Board, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, Version 1.0,

02.09.2020, abrufbar unter https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-072020-concepts-controller-and-processor_de.

EDSA Leitlinien 02/2018: Der Europäische Datenschutzausschuss, Leitlinien 2/2018 zu den Ausnahmen nach Artikel 49 der Verordnung 2016/679, angenommen am 25. Mai 2018, abrufbar unter https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_2_2018_derogations_de.pdf.

EDSB Microsoft Public Paper 02.07.2020: European Data Protection Supervisor, EDPS public paper on Outcome of own-initiative investigation into EU institutions' use of Microsoft products and services, 02.07.2020, abrufbar unter https://op.europa.eu/en/publication-detail/-/publication/ddc8842d-ca33-11ea-adf7-01aa75ed71a1/language-en.

EDSB Strategy Schrems II 30.10.2020: European Data Protection Supervisor, Strategy for Union institutions, offices, bodies and agencies to comply with the 'Schrems II' Ruling, 30.10.2020, abrufbar unter https://edps.europa.eu/sites/edp/files/publication/2020-10-29_edps_strategy_schremsii_en_0.pdf.

EDSB/EDSA Joint Opinion 14.01.2021: European Data Protection Supervisor / European Data Protection Board, Joint Opinion 2/2021 on standard contractual clauses for the transfer of personal data to third countries, 14.01.2021, abrufbar unter https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-22021-standard_de.

Ehmann/Selmayr-*Bearbeiter*: Eugen Ehmann, Martin Selmayr, DS-GVO. Datenschutz Grundverordnung. Kommentar, 2. Auflage 2018.

Engeler/Felber, ZD 2017, 251: Malte Engeler, Wolfram Felber, Entwurf der e-Privacy-VO aus der Perspektive der aufsichtsbehördlichen Praxis, in ZD 2017, S. 251–257.

Ermert heise.de 20.11.2020: Monika Ermert, EU-Verschlüsselungsdebatte: Die fixe Idee von der „magischen Lösung", 20.11.2020, abrufbar unter https://www.heise.de/news/EU-Verschluesselungsdebatte-Die-fixe-Idee-von-der-magischen-Loesung-4966595.html.

Ertel Blog 14.05.2020: Sebastian Ertel, Videokonferenzen mit BigBlueButton, 14.05.2020, abrufbar unter https://www.datenschutz-notizen.de/videokonferenzen-mit-bigbluebutton-5425839/.

Fennessy iapp Blog 11.11.2020: Caitlin Fennessy, A breakdown of EDPB's recommendations for data transfers post 'Schrems II', 11.11.2020, abrufbar unter https://iapp.org/news/a/a-break-down-of-edpbs-recommendations-for-data-transfers-post-schrems-ii/.

Fietkau/Renz/Trénel ZKM 2001, 132: Hans-Joachim Fietkau, Andrea Renz, Matthias Trénel, Online-Mediation in öffentlichen Konfliktlagen, in ZKM 2001, S. 132–125.

Frye/Simitis Forschung Frankfurt 2015, 44: Bernd Frye, Spiros Simitis, »Es geht um Eure Daten!« Hat der Datenschutz noch eine Chance? in Forschung Frankfurt 2015, S. 44–49, abrufbar unter https://www.forschung-frankfurt.uni-frankfurt.de/57255965.pdf.

Gal Zoom Blog 01.04.2020: Oded Gal, The Facts Around Zoom and Encryption for Meetings/Webinars, 01.04.2020, abrufbar unter https://blog.zoom.us/facts-around-zoom-encryption-for-meetings-webinars/.

GDD Praxishilfe DS-GVO XVI 4-2020: Gesellschaft für Datenschutz und Datensicherheit e.V., GDD-Praxishilfe DS-GVO XVI Videokonferenzen und Datenschutz, Stand April 2020, abrufbar unter https://www.gdd.de/downloads/praxishilfen/gdd-praxishilfe_xvi-videokonferenzen-und-datenschutz.

GDD Praxishilfe DS-GVO XVI Anlage II: Gesellschaft für Datenschutz und Datensicherheit e.V., GDD-Praxishilfe DS-GVO XVI Videokonferenzen und Datenschutz, Anlage II PH Videokonferenzsysteme Version 2.1, Januar 2021 (im Dokument angegeben als 07.Juni 2021), abrufbar unter https://www.gdd.de/downloads/praxishilfen/ph_videokonferenzsysteme_aktuelle-tabelle/view.

Gläßer/Sinemillioglu/Wendenburg ZKM 2020, 80: Ulla Gläßer, Nora Sevbihiv Sinemillioglu, Felix Wendenburg, Online-Mediation – Teil 1, in ZKM 2020, S. 80–85.

Gläßer/Sinemillioglu/Wendenburg ZKM 2020, 133: Ulla Gläßer, Nora Sevbihiv Sinemillioglu, Felix Wendenburg, Online-Mediation – Teil 2, in ZKM 2020, S. 133–138.

Gola-*Bearbeiter*: Peter Gola (Hrsg.), Datenschutz-Grundverordnung VO (EU) 2016/679. Kommentar, 2. Auflage 2018.

Grages CR-online.de Blog 12.11.2020: Jan-Michael Grages, Steine statt Brot: Empfehlungen des EDSA zu Datentransfers nach Schrems II, 12.11.2020, abrufbar unter https://www.cr-online.de/blog/2020/11/12/steine-statt-brot-empfehlungen-des-edsa-zu-datentransfers-nach-schrems-ii/.

Greger Stellungnahme MediationsG I: Reinhard Greger, Stellungnahme der Centrale für Mediation (CfM) zum Referentenentwurf des Bundesministeriums der Justiz Gesetz zur Förderung der Mediation und anderer Verfahren der außergerichtlichen Konfliktbeilegung (Mediationsgesetz) – Stand 04.08.2010 – abrufbar unter https://www.reinhard-greger.de/dateien/Stellungnahme_Centrale-fuer-Mediation.pdf.

Greger Stellungnahme MediationsG II : Reinhard Greger, Referentenentwurf eines Gesetzes zur Förderung der Mediation und anderer Verfahren zur außergerichtlichen Konfliktbeilegung (Mediationsgesetz) vom 04.08.2010 (zur Umsetzung der RL 2008/52/EG des Europäischen Parlaments und des Rates vom 21.05.2008) Stellungnahme des Anwaltsverbandes Baden-Württemberg im Deutschen Anwaltverein e.V. – vom 17.09.2010 – abrufbar unter https://www.reinhard-greger.de/dateien/Stellungnahme_Anwaltsverband-Baden-Wuerttemberg.pdf.

Greger/Unberath/Steffek-*Bearbeiter*: Reinhard Greger, Hannes Unberath (+), Felix Steffek, Recht der alternativen Konfliktlösung. Mediationsgesetz. Verbraucherstreitbeilegungsgesetz, 2. Auflage 2016.

Härting CR-online.de Blog 29.08.2018: Niko Härting, Warum ich keiner kleineren Arztpraxis oder Anwaltskanzlei die Bestellung eines Datenschutzbeauftragten empfehle, 29.08.2018, abrufbar unter https://www.cr-online.de/blog/2018/08/29/warum-ich-keiner-kleineren-arzpraxis-oder-anwaltskanzlei-die-bestellung-eines-datenschutzbeauftragten-empfehle/.

Härting beck-aktuell 24.08.2020: Niko Härting, Danke, Max Schrems!, 24.08.2020, abrufbar unter https://rsw.beck.de/aktuell/daily/magazin/detail/danke-max-schrems!.

Haft/Schlieffen-*Bearbeiter*: Fritjof Haft, Katharina Gräfin von Schlieffen (Hrsg.), Handbuch Mediation, 3. Auflage, 2016.

Heim Blog 24.07.2020: Jürgen Heim, Das neue Phänomen „Zoom Fatigue". Ursachen und Gegenstrategien, 24.07.2020, ursprünglich veröffentlicht unter https://www.mediationaktuell.de/news/neue-phaenomen-zoom-fatigue, inzwischen nur noch in archivierter Fassung, bspw. unter https://web.archive.org/web/20210224210914/https://www.mediationaktuell.de/news/neue-phaenomen-zoom-fatigue.

Hinterhölzl-Widi: Online-Mediation. Erweist sich Online-Mediation als taugliches Instrument in Österreich?, 2009, Wien, Österreich.

Hornung MMR 2004, 3: Gerrit Hornung, Zwei runde Geburtstage: Das Recht auf informationelle Selbstbestimmung und das WWW, in MMR 2004, S. 3–8.

John/Wellmann DuD 2020, 506: Nicolas John, Maximilian Wellmann, Datenschutzrechtliche Fragestellungen zur Auswahl von Videokonferenztools, in DuD 2020, S. 506–510.

John/Wellmann DuD 2020, 606: Nicolas John, Maximilian Wellmann, Datenschutzrechtliche Fragestellungen bei der Einrichtung und Verwendung von Videokonferenztools, in DuD 2020, S. 606–610.

Keppeler CR 2019, 18: Lutz Martin Keppeler, Warum Anwälte nach der DSGVO nicht (zwingend) Ende-zu-Ende verschlüsselt kommunizieren müssen. Praxisprobleme in der Anwendung von Art 32 DSGVO, in CR 2019, S. 18–24.

Kilburg Komet Blog 14.07.2020: Sascha Kilburg, Online-Moderation: Die Kommunikation zwischen den Beteiligten – Welche Tools eignen sich als virtueller Beratungsraum?, 14.07.2020, abrufbar unter http://komet-hamburg.de/mediationsnahe-verfahren/73/online-moderation-die-kommunikation-zwischen-den-beteiligten-welche-tools-eignen-sich-als-virtueller-beratungsraum.

Kiparski CR 2019, 460: Gerd Kiparski, Der EuGH schafft Klarheit: OTT-Dienste sind in der Regel keine Telekommunikationsdienste. Zugleich Anmerkung zu EuGH, Urt. v. 13.6.2019 – C193/18 (Google) und Urt., v. 5.6.2019 – C-142/18 (Skype), in CR 2019, S. 460–464.

Kiparski CR-online.de Blog 06.08.2020: Gerd Kiparski, Ein neues Datenschutz-Stammgesetz für den Telekommunikations. und Telemedien-Datenschutz: Das TTDSG, 06.08.2020, abrufbar unter https://www.cr-online.de/blog/2020/08/06/ein-neues-datenschutz-stammgesetz-fuer-den-telekommunikations-und-telemedien-datenschutz-das-ttdsg/.

Kiparski CR-online.de Blog 23.08.2020: Gerd Kiparski, Kundenschutz im neuen TKG, 23.08.2020, abrufbar unter https://www.cr-online.de/blog/2020/08/23/kundenschutz-im-neuen-tkg/.

Klowait/Gläßer-*Bearbeiter*: Jürgen Klowait, Ulla Gläßer (Hrsg.), Mediationsgesetz Handkommentar, 2. Auflage, 2018.

Kremer ITRB 2020, 35: Sascha Kremer, Unverschlüsselte E-Mail-Kommunikation mit Kunden und Mandaten. Datenschutz- oder berufsrechtliche Pflicht zur (aufgedrängten) E-Mail-Verschlüsselung?, ITRB 2020, S. 35–40.

Krempl heise.de 31.10.2020: Stefan Krempl, Baden-Württemberg: Test von Microsoft 365 an Schulen kann starten, 31.10.2020, abrufbar unter https://www.heise.de/news/Baden-Wuerttemberg-Test-von-Microsoft-365-an-Schulen-kann-starten-4944515.html.

Krempl heise.de 13.11.2020: Stefan Krempl, Terrorbekämpfung und Verschlüsselung: EU-Rat forciert die umstrittene Crypto-Linie, 13.11.2020, https://www.heise.de/news/Terrorbekaempfung-und-Verschluesselung-EU-Rat-forciert-umstrittene-Crypto-Linie-4960069.html.

Krempl heise.de 20.11.2020: Stefan Krempl, EU-Rat: Bundesregierung gibt bei der E-Privacy-Verordnung vorerst auf, 20.11.2020, abrufbar unter https://www.heise.de/news/EU-Rat-Bundesregierung-gibt-bei-der-E-Privacy-Verordnung-vorerst-auf-4967461.html.

Krempl heise.de 22.04.2021: Stefan Krempl, TKG-Novelle: Bundestag beschließt "schnelles" Internet für alle, 22.04.2021, https://www.heise.de/news/TKG-Novelle-Bundestag-beschliesst-schnelles-Internet-fuer-alle-6024446.html.

Krempl heise.de 07.05.2021: Stefan Krempl, TKG-Novelle: Bundesrat billigt "schnelles" Internet für alle mit Auflagen, 07.05.2021, https://www.heise.de/news/TKG-Novelle-Bundesrat-billigt-schnelles-Internet-fuer-alle-mit-Auflagen-6041456.html.

Kühling/Schall CR 2015, 641: Jürgen Kühling, Tobias Schall, WhatsApp, Skype & Co. – OTT-Kommunikationsdienste im Spiegel des geltenden Telekommunikationsrechts, in CR 2015, S. 641–655.

Kuketz Blog 16.04.2019: Mike Kuketz, Google Data Collection: Eine fundierte Analyse, 16.04.2019, abrufbar unter https://www.kuketz-blog.de/google-data-collection-eine-fundierte-analyse/.

LDA Bayern, LfDI BW PM 02.10.2020: Stefan Brink, Thomas Petri, Michael Will et. al., Gemeinsame Pressemitteilung zu Microsoft Office 365. Microsoft Office 365: Bewertung der Datenschutzkonferenz zu undifferenziert – Nachbesserungen gleichwohl geboten, 02.10.2020, abrufbar u. a. unter https://www.baden-wuerttemberg.datenschutz.de/gemeinsame-pressemitteilung-zu-microsoft-office-365/.

LfDI BW OH VK 07.09.2020: Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg, Orientierungshilfe des LfDI BW: Was jetzt in Sachen internationaler Datentransfer?, 2. Auflage 07.09.2020, abrufbar unter https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2020/08/Orientierungshilfe-Was-jetzt-in-Sachen-internationaler-Datentransfer.pdf.

LfDI BW PM 17.04.2020: Landesbeauftragter für den Datenschutz und die Informationsfreiheit Baden-Württemberg, Datenschutzfreundliche technische Möglichkeiten der Kommunikation, Pressemeldung vom 17.04.2020, abrufbar unter https://www.baden-wuerttemberg.datenschutz.de/datenschutzfreundliche-technische-moeglichkeiten-der-kommunikation/.

LfDI BW PM 30.10.2020: Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg, LfDI begleitet Pilotprojekt des Kultusministeriums zur Nutzung von Microsoft Office 365 an Schulen, 30.10.2020, abrufbar unter https://www.baden-wuerttemberg.datenschutz.de/lfdi-begleitet-pilotprojekt-des-kultusministeriums-zur-nutzung-von-microsoft-office-365-an-schulen/.

LfDI BW PM 20.11.2020: Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg, #DSGVOwirkt: Microsoft passt sich europäischem Datenschutz an, 20.11.2020, abrufbar unter https://www.baden-wuerttemberg.datenschutz.de/dsgvowirkt/.

LfDI BW PM 07.05.2021: Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg, Empfehlung des LfDI hinsichtlich der Nutzung der geprüften Version von Microsoft Office 365 an Schulen, 07.05.2021, abrufbar unter https://www.baden-wuerttemberg.datenschutz.de/lfdi-raet-aufgrund-hoher-datenschutzrechtlicher-risiken-von-der-nutzung-der-gepruefte-version-von-microsoft-office-365-an-schulen-ab/.

LfD Nds FAQ VK 8-2020: Die Landesbeauftragte für den Datenschutz Niedersachsen, Fragen und Antworten zu Videokonferenzsystemen (August 2020), abrufbar unter https://lfd.niedersachsen.de/download/158091.

Löer ZKM 2010, 179: Lambert Löer, Referentenentwurf eines Mediationsgesetzes – Eine Stellungnahme aus der Sicht eines zivilgerichtlichen Richtermediatoren –, in ZKM 2010, S. 179–182.

Loock-Wagner ZKM 2002, 206: Oliver Loock-Wagner, Online-Mediation, quo vadis?, in ZKM 2002, S. 206–209.

Lütkehaus ZKM 2020, 102: Isabell Lütkehaus, „Ich kann dich nicht riechen". Ein Plädoyer für die Mediation im virtuellen Raum, in ZKM 2020, S. 102–104.

Michl DuD 2017, 349: Walther Michl, Das Verhältnis zwischen Art. 7 und Art. 8 GRCh – zur Bestimmung der Grundlage des Datenschutzgrundrechts im EU-Recht, in DuD 2017, S. 349–353.

Moechel ORF 08.11.2020: Erich Moechel, Auf den Terroranschlag folgt EU-Verschlüsselungsverbot, 08.11.2020, abrufbar unter https://fm4.orf.at/stories/3008930/.

MüKo ZPO-*Bearbeiter*: Wolfgang Krüger, Thomas Rauscher (Hrsg.), Münchener Kommentar zur Zivilprozessordnung, Band 1, 6. Auflage 2020.

Neuerer handelsblatt.de 03.05.2021: Dietmar Neuerer, Streit über Cloud-Nutzung in den USA – Wirtschaft sendet Hilferuf an die Bundesregierung, 03.05.2021, abrufbar unter https://www.handelsblatt.com/politik/deutschland/brief-an-die-bundesregierung-streit-ueber-cloud-nutzung-in-den-usa-wirtschaft-sendet-hilferuf-an-die-bundesregierung/27151300.html.

Neuerer handelsblatt.de 08.05.2021: Dietmar Neuerer, Riskanter Datenaustausch mit den USA: Unternehmen fordern in einem Brief Hilfe von Brüssel, 08.05.2021, abrufbar unter https://www.handelsblatt.com/politik/deutsch-

land/transatlantischer-datenverkehr-riskanter-datenaustausch-mit-den-usa-unternehmen-fordern-in-einem-brief-hilfe-von-bruessel/27172556.html?ticket=ST-4741645-uPBZaNMkMO4WxD95kqyl-ap2.

Papier Vortrag 2010: Hans-Jürgen Papier, Entwicklungen des Rechts auf informationelle Selbstbestimmung seit dem Volkszählungsurteil des Bundesverfassungsgerichts, Vortrag im Rahmen der 1. Bitburger Gespräche. München, 14.–15. Oktober 2010, abrufbar auf der Übersichtsseite unter https://www.uni-trier.de/universitaet/fachbereiche-faecher/fachbereich-v/forschung/institute-und-forschungsstellen/irp/publikationen/jahrbuecher-bitburger-gespraeche-1/beitraege-1-bitburger-gespraeche-in-muenchen.

Piltz/Hessel Reuschlaw Blog 4-2020: Carlo Piltz, Stefan Hessel, Berliner Datenschutzaufsicht: Stellungnahme und Checkliste zum Datenschutz bei Videokonferenzen, Dienstleistungen von Microsoft (insb. Teams und Skype) sowie Zoom sind nicht datenschutzgerecht, April 2020, abrufbar unter https://www.reuschlaw.de/news/berliner-datenschutzaufsicht-stellungnahme-und-checkliste-zum-datenschutz-bei-videokonferenzen/.

Rickert ZKM 2009, 168: Anne Rickert, Online-Mediation im virtuellen Raum, in ZKM 2009, S. 168–172.

Rickert KD 2019, 64: Anne Rickert, Live-Online-Mediation – ein Zukunftstrend?, in KD 2019, S. 64–71.

RTMKM ZKM 2009, 147: Round Table ‚Mediation & Konfliktmanagement' der Deutschen Wirtschaft, Positionspapier der deutschen Wirtschaft zur Umsetzung der EU-Mediationsrichtlinie, in ZKM 2009, S. 147–153.

Schertz Vortrag 2013: Christian Schertz, Der Verlust der Privatsphäre in der modernen Mediengesellschaft – Ist das Individuum noch geschützt?, Vortrag im Rahmen der 56. Bitburger Gespräche. Mainz, 10.–11.01.2013, abrufbar auf der Übersichtsseite unter https://www.uni-trier.de/universitaet/fachbereiche-faecher/fachbereich-v/forschung/institute-und-forschungsstellen/irp/publikationen/jahrbuecher-bitburger-gespraeche-1/beitraege-56-bitburger-gespraeche.

Sassenberg/Franke CR 2013, 772: Die regulatorische Einordnung der Videokonferenz. Wann das Angebot von Videotelefonie wesentliche telekommunikationsrechtliche Pflichten auslöst, in CR 2013, S. 772–779.

Schmidt-*Bearbeiter*: Hubert Schmidt (Hrsg.), COVID-19. Rechtsfragen zur Corona-Krise, 2. Auflage 2020.

Schuster/Grützmacher-*Bearbeiter*: Fabian Schuster, Malte Grützmacher (Hrsg.), IT-Recht. Kommentar, 1. Auflage 2020.

Schwitteck/von Baumbach ZKM 2020, 104: Eva Schwittek, Christian von Baumbach, Konfliktbearbeitung über Distanz. Online-Mediation – Ein Erfahrungsaustausch unter Kollegen, in ZKM 2020, S. 104–106.

Sehl LTO Blog 21.10.2020: Markus Sehl, Gesetzgeber setzt BVerfG-BND-Urteil um. Internationale Überwachungsregeln made in Karlsruhe?, 21.10.2020, abrufbar unter https://www.lto.de/recht/hintergruende/h/bverfg-bnd-gesetzgeber-ueberwachung-geheimdienst-ausland-grundrechte-international-europa-eugh-schrems/.

Simitis/Hornung/Spiecker-*Bearbeiter*: Spiros Simitis, Gerrit Hornung, Indra Spiecker gen. Döhmann, Datenschutzrecht. DSGVO mit BDSG, 1. Auflage 2019.

Sokolov heise.de 09.11.2020: Daniel AJ Sokolov, EU-Regierungen planen Verbot sicherer Verschlüsselung, heise.de 09.11.2020, abrufbar unter https://www.heise.de/hintergrund/EU-Regierungen-planen-Verbot-sicherer-Verschluesselung-4951415.html.

Spindler, Gerichtsnahe Mediation: Gerald Spindler, Gerichtsnahe Mediation in Niedersachsen. Eine juristisch-rechtsökonomische Analyse. Abschlussbericht im Auftrag des Niedersächsischen Ministeriums für Justiz und des Niedersächsischen Ministeriums für Wissenschaft und Kultur, abrufbar unter https://www.univerlag.uni-goettingen.de/bitstream/handle/3/isbn-3-938616-67-9/mediation.pdf;jsessionid=0ED92A7D44EB43F6235FA8B60C02A4C5?sequence=1.

Spivak Wired 2013: Nova Spivak, The Post-Privacy World. Blog Entry, Juli 2013, abrufbar unter https://www.wired.com/insights/2013/07/the-post-privacy-world/.

Troja ZKM 2009, 152: Markus Troja, Lehrmodul 13: Vorbereitung und Mediationsvertrag – Die erste Phase eines Mediationsverfahrens – , in ZKM 2009, S. 152–157.

US DOC SCC Whitepaper: US Department of Commerce, Information on U.S. Privacy Safeguards Relevant to SCCs and Other EU Legal Bases for EU-U.S. Data Transfers after Schrems II. Whitepaper. September 2020, abrufbar unter https://www.commerce.gov/sites/default/files/2020-09/SCCsWhitePaperFORMATTEDFINAL508COMPLIANT.PDF.

US DOJ CLOUD Act Whitepaper: US Department of Justice, Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act. White Paper. April 2019, abrufbar unter https://www.justice.gov/opa/press-release/file/1153446/download.

Veil CR-online.de Blog, 22.04.2021: Winfried Veil, Zum Schutzgut der DSGVO: Eine naive Wortlautanalyse, 22.04.2021, abrufbar unter https://www.cr-online.de/blog/2021/04/22/zum-schutzgut-der-ds-gvo-eine-naive-wortlautanalyse/.

Wacker ZKM 2001, 265: Ulf Wacker, Online-Mediation, in ZKM 2001, S. 265–269.

Wagner ZKM 2010, 172: Gerhard Wagner, Der Referentenentwurf eines Mediationsgesetzes, in ZKM 2010, S. 172–176.

Wagner ZKM 2011, 164: Gerhard Wagner, Vertraulichkeit der Mediation, in ZKM 2011, S. 164–168.

WAR-Stellungnahme: Bernd Holznagel, Frank Brettschneider *et.al.*, Wissenschaftlicher Arbeitskreis für Regulierungsfragen (WAR) bei der Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen, Fragen der Regulierung von OTT-Kommunikationsdiensten, 15.07.2016, abrufbar unter https://www.bundesnetzagentur.de/DE/Allgemeines/DieBundesnetzagentur/WAR/Stellungnahmen/Stellungnahme_OTT.pdf?__blob=publicationFile&v=2.

Weigel NJOZ 2015, 41: Christoph Weigel, Die Absicherung der Vertraulichkeit in der Mediation, in NJOZ 2015, S. 41–44.

Weigel Inkovema Blog 17.02.2020: Sascha Weigel, Datenschutz für selbständige Mediator*innen. Was selbständige Mediator*innen beachten müssen, um datenschutzkonform zu arbeiten, 17.02.2020, abrufbar unter https://inkovema.de/blog/datenschutz-fuer-mediatorinnen/.

Wilkens heise.de 07.05.2021: Andreas Wilkens, Microsoft 365 an Schulen: Baden-Württembergs Datenschutzbeauftragter rät ab, 07.05.2021, abrufbar unter https://www.heise.de/news/Microsoft-365-an-Schulen-Baden-Wuerttembergs-Datenschutzbeauftragter-raet-ab-6041379.html.

Zöller ZPO-*Bearbeiter*: Richard Zöller (Begr.), Zivilprozessordnung, Kommentar, 33. Auflage, 2020.

Zoom Whitepaper E2E Encryption: Josh Blum, Simon Booth, et. al., E2E Encryption for Zoom Meetings, Version 3, 15.12.2020, abrufbar unter https://github.com/zoom/zoom-e2e-whitepaper/blob/master/zoom_e2e.pdf.

Alle im Literaturverzeichnis, im Abkürzungsverzeichnis / Glossar sowie in den Fußnoten angegebenen Webseiten wurden am 13.05.2021 zuletzt aufgerufen. Datumsangaben im Literaturverzeichnis sowie in den Fußnoten beziehen sich nicht auf das Datum des letzten Zugriffs, sondern auf das Veröffentlichungsdatum.

Abkürzungsverzeichnis und Glossar

A

a. F.	alte Fassung
Abs.	Absatz
AEMR	Allgemeine Erklärung der Menschenrechte, Universal Declaration of Human Rights (UDHR), verabschiedet als Resolution durch die UN Generalversammlung am 10. Dezember 1948, http://www.un-documents.net/a3r217.htm#A
AEUV	Konsolidierte Fassung des Vertrags über die Arbeitsweise der Europäischen Union 2012/C 326/01, https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=celex%3A12012E%2FTXT
Anh.	Anhang
Art.	Artikel
Artt.	Artikel (pl.)
Art. 29-DSG	Artikel-29-Datenschutzgruppe, Article 29 Working Party, abgelöst seit dem 25.08.2018 durch den EDSA, https://ec.europa.eu/newsroom/article29/news.cfm?item_type=1358
AVV	Auftragsverarbeitungsvereinbarung (Art. 28 Abs. 3 DSGVO)

B

BBDI	Berliner Beauftragte für den Datenschutz und die Informationsfreiheit, https://www.datenschutz-berlin.de/
BDSG*	Bundesdatenschutzgesetz
BGB*	Bürgerliches Gesetzbuch
BGBl.	Bundesgesetzblatt, https://www.bgbl.de/xaver/bgbl/start.xav#__bgbl__%2F%2F*%5B%40attr_id%3D%27I_2020_52_inhaltsverz%27%5D__1605883596936
BGH	Bundesgerichtshof der Bundesrepublik Deutschland, https://www.bundesgerichtshof.de/DE/Home/home_node.html

BGHZ	Entscheidungen des Bundesgerichtshofs in Zivilsachen, herausgegeben von Mitgliedern des Bundesgerichtshofs und der Bundesanwaltschaft, zitiert nach Band, Seite
BMJV	Bundesministerium für Justiz und Verbraucherschutz, https://www.bmjv.de/DE/Startseite/Startseite_node.html
BMWi	Bundesministerium für Wirtschaft und Energie, https://www.bmwi.de/Navigation/DE/Home/home.html
BNetzA	Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen, https://www.bundesnetzagentur.de/DE/Home/home_node.html
bspw.	beispielsweise
BT-Drs	Bundestags-Drucksache, http://dipbt.bundestag.de/dip21.web/bt
BVerfGE	Entscheidungen des Bundesverfassungsgerichts, herausgegeben vom Verein der Richter des Bundesverfassungsgerichts, zitiert nach Band, Seite und ggf. Randnummer, https://www.bundesverfassungsgericht.de/DE/Entscheidungen/Entscheidungen/Amtliche%20Sammlung%20BverfGE.html
bzw.	beziehungsweise

C

CEP	Centrum für Europäische Politik, https://www.cep.eu/de.html.
CLOUD Act	Clarifying Lawful Overseas Use of Data Act der USA, March 21, 2018, pages 2201–2232, https://www.justice.gov/dag/page/file/1152896/download
CR	Computer und Recht, Zeitschrift

D

d. h.	das heißt
Datenschutz-RL	Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr,

	https://eur-lex.europa.eu/eli/dir/1995/46/oj?locale=de aufgehoben durch die DSGVO
DAV	Deutscher Anwaltverein, https://anwaltverein.de/de
DIHK	Deutscher Industrie- und Handelskammertag e.V., https://www.dihk.de/de
DSB	Datenschutzbeauftragter
DSG-CH	Bundesgesetz über den Datenschutz (DSG) vom 19. Juni 1992 (Stand am 1. März 2019) der Bundesversammlung der Schweizerischen Eidgenossenschaft, https://www.admin.ch/opc/de/classified-compilation/19920153/index.html
DSGVO	Europäische Datenschutzgrundverordnung, Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=celex%3A32016R0679
DSK	Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder, https://www.datenschutzkonferenz-online.de
DSMV	Landesbeauftragter für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern, https://www.datenschutz-mv.de/
DuD	Datenschutz und Datensicherheit, Zeitschrift

E

EDPB	Siehe EDSA
EDPS	Siehe EDSB
EDSA	Europäischer Datenschutzausschuss, European Data Protection Board (EDPB), bestehend aus Vertretern der nationalen Datenschutzbehörden und dem EDSB, https://edpb.europa.eu/edpb_de

EDSB	Europäischer Datenschutzbeauftragter, European Data Protection Supervisor (EDPS), die unabhängige Datenschutzbehörde der EU https://edps.europa.eu/edps-homepage_de
EECC	European Electronic Communications Code – Europäischer Kodex für Elektronische Kommunikation, Richtlinie (EU) 2018/1972 des Europäischen Parlaments und des Rates vom 11. Dezember 2018 über den europäischen Kodex für die elektronische Kommunikation (Neufassung), https://eur-lex.europa.eu/legal-content/DE/TXT/?qid=1602501691550&uri=CELEX:32018L1972 mit Berichtigung vom 27.12.2019 unter https://eur-lex.europa.eu/legal-content/DE/TXT/?qid=1602501691550&uri=CELEX:32018L1972R(01)
EG	Erwägungsgrund
Einl.	Einleitung
EMRK	Europäische Menschenrechtskonvention, Convention for the Protection of Human Rights and Fundamental Freedoms, in Kraft getreten am 3 September 1953, veröffentlicht auf den Seiten des Europarates unter https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/005
ePrivacy-RL	Richtlinie 2009/136/EG des Europäischen Parlaments und des Rates vom 25. November 2009 zur Änderung der Richtlinie 2002/22/EG über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten, der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation und der Verordnung (EG) Nr. 2006/2004 über die Zusammenarbeit im Verbraucherschutz, abrufbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A02009L0136-20091219#
ePrivacy-VO	Geplante Verordnung: Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG (Verordnung

	über Privatsphäre und elektronische Kommunikation), 2017/0003 (COD), initialer Entwurf vom 10.01.2017, abrufbar unter https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-privacy-and-electronic-communications, inzwischen diverse Überarbeitungsvorschläge, zuletzt am 4.11.2020 durch den Vorschlag der deutschen Ratspräsidentschaft unter https://data.consilium.europa.eu/doc/document/ST-9931-2020-INIT/en/pdf
et. al.	et alii / et aliae / et alia, und andere
EU	Europäische Union
EU DSS-Beschluss	EU Datenschutzschild (auch Privacy Shield genannt), Durchführungsbeschluss (EU) 2016/1250 der Kommission vom 12. Juli 2016 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des vom EU-US-Datenschutzschild gebotenen Schutzes, (in EU Dokumenten auch „DSS-Beschluss“ genannt) abrufbar unter https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.207.01.0001.01.ENG
EU SDK	EU Standarddatenschutzklauseln (auch Standardvertragsklauseln, Standard Contractual Clauses, SCC genannt), Beschluss 2010/87/EU der Kommission vom 5. Februar 2010 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern nach der Richtlinie 95/46 (Abl. 2010, L 39, S. 5) abrufbar unter https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32010D0087, in der durch den Durchführungsbeschluss (EU) 2016/2297 der Kommission vom 16. Dezember 2016 (Abl. 2016, L 344, S. 100) geänderten Fassung abrufbar unter https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02010D0087-20161217 Zuletzt neugefasst durch den Durchführungsbeschluss der EU Kommission vom 12.11.2020, Commission Implementing Decision on standard contractual clauses for the transfer of personal data to third countries, abrufbar im Rahmen der öffentlichen Konsultation unter

	https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12741-Commission-Implementing-Decision-on-standard-contractual-clauses-for-the-transfer-of-personal-data-to-third-countries
EU-USA Rechtshilfeabkommen	Abkommen zwischen der Europäischen Union und den Vereinigten Staaten von Amerika über Rechtshilfe, EUR-Lex – 22003A0719(02) – EN, vom 19.07.2003, abrufbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=celex%3A22003A0719%2802%29
EuGH	Gerichtshof der Europäischen Union, https://europa.eu/european-union/about-eu/institutions-bodies/court-justice_de
EuZW	Europäische Zeitschrift für Wirtschaftsrecht
EWR	Europäischer Wirtschaftsraum, gegründet durch das EWR-Abkommen, umfasst derzeit neben allen Mitgliedsstaaten der EU auch Island, Liechtenstein sowie Norwegen
EWR-Abkommen	Abkommen über den Europäischen Wirtschaftsraum, siehe übergreifende Webseite der EU unter https://eur-lex.europa.eu/legal-content/DE/ALL/?uri=CELEX%3A21994A0103%2801%29

F

f.	und der/die folgende
Fa.	Firma
ff.	und die folgenden
Fn.	Fußnote

G

GDD	Gesellschaft für Datenschutz und Datensicherheit e. V., https://www.gdd.de/
GG*	Grundgesetz
ggf.	gegebenenfalls
GmbH	Gesellschaft mit beschränkter Haftung

GRCh	Charta der Grundrechte der Europäischen Union, Charter of Fundamental Rights of the European Union, vom 26.10.2012, https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:12012P/TXT

H

Hrsg.	Herausgeber

I

i.d.R:	in der Regel
ICC	International Chamber of Commerce – Internationale Handelskammer, https://iccwbo.org/
IDR	Journal of international dispute resolution
insbes.	insbesondere
IP	Internet Protocol
IT	Informationstechnologie

J

JI-RL	Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates, https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=uriserv%3AOJ.L_.2016.119.01.0089.01.DEU

K

KD	Konfliktdynamik, Zeitschrift

L

LDA Bayern	Bayerisches Landesamt für Datenschutzaufsicht, https://www.lda.bayern.de/de/index.html.
LfDI BW	Landesbeauftragter für den Datenschutz und Informationsfreiheit Baden-Württemberg, https://www.baden-wuerttemberg.datenschutz.de/
LfD Nds	Landesbeauftragte für den Datenschutz Niedersachsen, https://lfd.niedersachsen.de/startseite/
lit.	Buchstabe
LLC	Limited liability companiy, Gesellschaft mit beschränkter Haftung (USA)

M

m. w. N.	mit weiteren Nachweisen
MediationsG*	Gesetz zur Förderung der Mediation und anderer Verfahren der außergerichtlichen Konfliktbeilegung
Mediations-RL	Richtlinie 2008/52/EG des Europäischen Parlaments und des Rates vom 21. Mai 2008 über bestimmte Aspekte der Mediation in Zivil- und Handelssachen, deutsche Sprachfassung unter https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:136:0003:0008:DE:PDF
MMR	Multimedia und Recht, Zeitschrift

N

NJOZ	Neue Juristische Online Zeitschrift
Nr.	Nummer

O

OH	Orientierungshilfe

P

PM	Pressemeldung

R

Rn.	Randnummer
RTMKM	Round Table Mediation und Konfliktmanagement der deutschen Wirtschaft (RTMKM), https://www.rtmkm.de/

S

S.	Satz (bei Gesetzen), Seite (bei Veröffentlichungen)
s. o.	siehe oben
s. u.	siehe unten
Safe Harbor Pakt	Entscheidung der Kommission vom 26. Juli 2000 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des von den Grundsätzen des „sicheren Hafens" und der diesbezüglichen „Häufig gestellten Fragen" (FAQ) gewährleisteten Schutzes, vorgelegt vom Handelsministerium der USA, 25.08.2000, abrufbar unter https://eur-lex.europa.eu/legal-content/de/TXT/?uri=CELEX%3A32000D0520
sog.	sogenannt(e/er/es)
StGB*	Strafgesetzbuch

T

TKG*	Telekommunikationsgesetz
TKMoG-E	Entwurf eines Gesetzes zur Umsetzung der Richtlinie (EU) 2018/1972 des Europäischen Parlaments und des Rates vom 11. Dezember 2018 über den europäischen Kodex für die elektronische Kommunikation (Neufassung) und zur Modernisierung des Telekommunikationsrechts (Telekommunikationsmodernisierungsgesetz), BT-Drs 19/26108, 19/26964, 19/27035, 19/28865; aktueller Gesetzgebungsstand: https://dip21.bundestag.de/dip21/btd/19/288/1928865.pdf und Beschluss des Bundesrats, 07.05.2021, https://www.bundesrat.de/SharedDocs/drucksachen/2021/0301-0400/325-21(B).pdf?__blob=publicationFile&v=1, geplantes Inkrafttreten 31.12.2021.

TTDSG-E	Entwurf eines Gesetzes zur Regelung des Datenschutzes und des Schutzes der Privatsphäre in der Telekommunikation und bei Telemedien (Telemedien-Telekommunikations-Datenschutzgesetz), BT-Drs 19/27441, aktueller Gesetzgebungsstand: Öffentliche Anhörung im Ausschuss für Wirtschaft und Energie, 21.04.2021, m. w. N. unter https://www.bundestag.de/resource/blob/834702/8bac16ade11c8a68231a86ed753b3e64/to_116_21-04-2021_oeA-TTDSG-data.pdf. und https://www.bundestag.de/presse/hib/836284-836284.

U

u.	und
u. a.	unter anderem
u. U.	unter Umständen
UA	Unterabsatz
UNCITRAL	United Nations Commission on International Trade law – Kommission der Vereinten Nationen für internationales Handelsrecht, https://uncitral.un.org/en
US DOC	United States Department of Commerce, Handelsministerium der USA, https://www.commerce.gov/
US DOJ	United States Department of Justice, Justizministerium der USA, https://www.justice.gov/
USA	United States of America, Vereinigte Staaten von Amerika

V

VZG 1983*	Gesetz über eine Volks-, Berufs-, Wohnungs- und Arbeitsstättenzählung (Volkszählungsgesetz 1983) vom 25.03.1982

Z

z. B.	zum Beispiel
ZD	Zeitschrift für den Datenschutz
Ziff.	Ziffer
ZKM	Zeitschrift für Konfliktmanagement, Zeitschrift

ZMediatAusbV*	Verordnung über die Aus- und Fortbildung von zertifizierten Mediatoren (Zertifizierte-Mediatoren-Ausbildungsverordnung)
ZPO*	Zivilprozessordnung

*alle Gesetze und Verordnungen der Bundesrepublik Deutschland zitiert nach https://dejure.org/gesetze.

Alle Links hierin wurden zuletzt abgerufen am 13.05.2021.

Übersicht der Anhänge

Anhang 1 – Checkliste für die Dienstauswahl

Der Mediator, der sich für einen Videokonferenzdienst entscheidet, sollte seinen konkreten Funktionsbedarf bestimmen und bei seiner Auswahlentscheidung durch Prüfen, Testen und / oder eine Anfrage beim Anbieter validieren.

Allgemeine Kriterien	**Ja**	**Nein**	**Zu klären**
Vergütung (ggf. Höhe)			
u.U. verschiedene Funktions- und Vergütungsmodelle nebeneinander stellen			
Keine Begrenzung in der Laufzeit der Sitzung			
Begrenzung der Teilnehmerzahl akzeptabel			

Funktionale Kriterien	**Must have**	**Should have**	**Could have(*)**	**Ja**	**Nein**	**Zu klären**
Zusätzliche Moderatoren-Rollen						
HD Sprach- und Video wiedergabe						
Automatische Sprecher-ansicht						
Break-Out Räume						
Chat-Funktion						
Private Chat-Funktion						
Bildschirmfreigabe für den Organisator						
Bildschirmfreigabe für Teilnehmer						
Whiteboard						
Lokale Speicherung						
Aufzeichnung						
Zentraler Speicherplatz beim Anbieter						
Einbindung in Kalender						
Nutzung über Browser						
Nutzung mit Anwendung						
Weitere Features						

Anforderungen an die Qualität	**Must have**	**Should have**	**Could have(*)**	**Selbst zu definieren**		
Einfachheit der Bedienung				*Eigene Einschätzung*		
Komfort der Bedienung				*Eigene Einschätzung*		
Übertragungsqualität				*Zu testen*		
Anforderungen an Endgeräte				*Zu testen*		
Weitere Anforderungen						
Anforderungen an Vertraulichkeit und Datenschutz						
Geografie				**DE**	**EWR+ (**)**	**USA, global**
Sitz des Anbieters						
Standort der Server						
Unterauftragsverarbeiter (Subprocessors)						
Verarbeitungsort						
Sicherheit bei der Einwahl	**Must have**	**Should have**	**Could have(*)**	**Ja**	**Nein**	**Zu klären**
Generischer Weblink						
Passwort oder PIN für Zutritt						
Zwei-Faktor-Authentifizierung						
Rollenkonzept für Moderator und Gäste						
Waiting Room						
Kein Zutritt für Teilnehmer vor Konferenzeröffnung						
Verschließen nach Einwahl aller Teilnehmer						
Ggf. weitere Funktionen						

Sicherheit beim Betrieb	Must have	Should have	Could have(*)	Ja	Nein	Zu klären
Transport-Verschlüsselung						
Ende-zu-Ende-Verschlüsselung						
Verschlüsselung zentral gespeicherter Inhalte						
Ggf. weitere Zusagen und Funktionen						

AVV: Wesentliche Anforderungen	Ja	Nein	Zu klären
AVV vorhanden			
Auftrag klar geregelt			
Art der Daten bestimmt			
Kategorien der Betroffenen bestimmt			
Verarbeitungsarten bestimmt			
Verarbeitungsdauer bestimmt			
Verarbeitungszweck bestimmt			
Löschung nach Auftragsbeendigung vorgesehen			
Weisungsgebundenheit geregelt			
Vertraulichkeit (auch Hilfspersonen) geregelt			
Unterstützung des Verantwortlichen bei dessen datenschutzrechtlichen Pflichten			
Unterstützung bei Pflichten gegenüber Betroffenen und Aufsichtsbehörden			
Datenschutzbeauftragter benannt			
Ausreichende technische und org. Maßnahmen			
Berichtigung, Löschung, Sperrung der Daten geregelt			
Unterauftragsverarbeiter (Zustimmung/Einspruch)			
Auditrecht vorgesehen			
Mitteilungspflichten bei Datenschutzverletzungen			
Zusätzl. Verarbeitungen gem. Art. 6 (1) (f) DSGVO			
Zusätzliche Verarbeitungen aufgrund geltenden Rechts nur der EU und ihrer Mitgliedstaaten			

(*) Die Kategorie „Would Have“ bleibt hier praktischerweise unberücksichtigt.
(**) EWR+ steht für EWR und Staaten, für die ein Angemessenheitsbeschluss gem. Art. 45 DSGVO vorliegt.

Anhang 2 – Praktische Hinweise

Hinweise für die Organisation und Durchführung der Videokonferenz

- Bei der Toolauswahl nach der Checkliste vorgehen. Nur erforderliche Funktionalitäten wählen.
- Beim Aufsetzen der Konferenz bereits die Möglichkeit der Aufzeichnung deaktivieren. Eine Aufzeichnung der Videokonferenz läuft der Vertraulichkeit der Mediation zuwider.
- Verhaltensüberwachung ausschalten. Soweit das gewählte Videokonferenztool ein Aufmerksamkeitstracking (Aktivität des Anwendungsfensters) vorsieht, ist darauf zu achten, dass es nicht aktiviert ist.
- Moderator. Bei Großverfahren mit vielen Beteiligten ist eine Co-Moderatorenfunktion wichtig.
- Zugangsdaten mit Passwort. Nur die Medianden erhalten mit der Einladung die Zugangsdaten. Die Sitzung muss passwortgeschützt sein. Bei besondere Vertraulichkeit bieten manche Anbieter eine Zwei-Faktor-Authentifizierung.
- Warteraumfunktionalität. Soweit das gewählte Videokonferenztool über einen „Waiting Room“ verfügt, ist dieser zur Einlasskontrolle zu verwenden, damit nur die Eingeladenen den virtuellen Konferenzraum betreten. Soweit kein Warteraum vorhanden ist, muss der Mediator als erster den Raum betreten.
- Raum schließen. Der virtuelle Konferenzraum kann bei einigen Anbietern nach dem Beitritt aller Teilnehmer geschlossen werden, um den Zutritt Dritter auszuschließen.
- Keine Speicherung außer mit Einwilligung der Medianden. Es kann sinnvoll sein, während der Mediation erstellte Visualisierungen zu speichern und den Parteien zu überlassen. Ansonsten sollten alle Daten, inkl. Chatverläufe – auch seitens des Dienstanbieters – nach dem Konferenzende gelöscht werden.
- Gesicherte Aufbewahrung. Ist eine Verwendung der Visualisierungen in der nächsten Sitzung gewünscht, hat der Mediator sie bis dahin geschützt aufzubewahren.
- Einzelgespräche. Mit Einwilligung aller Beteiligten kann der Mediator Einzelgespräche während der Videokonferenz durch sog. Break-Out-Rooms organisieren.
- Beenden der Konferenz. Nach dem Abschluss der Sitzung sollte der Mediator darauf achten, dass nicht nur er den Raum verlässt, sondern die Sitzung für alle beendet.

Hinweise an die Teilnehmer

- Teilnahme ohne Login. Der Mediator sollte den Parteien datensparsame Zugangsmöglichkeiten empfehlen (kein Login über Facebook oder Google-Konto, sondern nur über den Browser, ggf. im Inkognito-Modus)
- Keine Weiterleitung. Die Teilnahmeinformationen dürfen nicht weitergeleitet werden.
- Teilnahme mit Klarnamen. Die Teilnehmer sollten nicht mit Pseudonymen oder Gerätenamen angezeigt werden, sondern ihre vollständigen Namen eintragen.
- Virtuelle Hintergründe und Blurring. Die Teilnehmer können zum Schutz ihrer Privatsphäre bei den meisten Tools ihren Wohnraum / ihren Arbeitsplatz im Hintergrund überdecken. Hierzu zählt auch eine entsprechende Prüfung und Anpassung des Kamerasichtfelds. Der Mediator sollte sie darauf hinweisen und ihnen die Einstellmöglichkeit erläutern.
- Identifikation. Zu Beginn der Sitzung sollten sich die Teilnehmer mit eingeschalteter Kamera kurz vorstellen.
- Videoübertragung. Während der Sitzung sollten die Teilnehmer ihre Kamera grundsätzlich anlassen.
- Keine weiteren Teilnehmer vor Ort. Während der Sitzung sollte sich die Beteiligten jeweils alleine im Raum befinden, die Tür schließen und bestenfalls mit Kopfhörern teilnehmen, um die Vertraulichkeit zu gewährleisten.
- Screenshots und Aufzeichnungen durch die Parteien sind nicht zulässig.

Anhang 3 – Beispiel einer Datenschutzerklärung für die Medianden

Dieser Anhang kann als Ausgangspunkt für eine Datenschutzinformation des Mediators an die Parteien dienen. Im Einzelfall ist zu prüfen, ob die hierin enthaltenen Informationen einschlägig, geeignet und ausreichend sind, und ggf. weitere Informationen zu ergänzen.

Datenschutzhinweise für die Durchführung einer Online-Mediation via Videokonferenz des *Name / Firma des Mediators.*

Hiermit möchte ich Sie als Teilnehmer der Online-Mediation über die Verarbeitung personenbezogener Daten (nachfolgend „Datenverarbeitung") im Rahmen des Mediationsverfahrens über Videokonferenz informieren.

1) Zweck der Verarbeitung

Ich nutze das Tool „*Name des Videokonferenzdienstes*" (nachfolgend: „VK-Dienst") der Firma „*Name der Anbieterfirma*" („nachfolgend: „VK-Anbieter") mit Sitz in *Anschrift einfügen*, um das Online-Mediationsverfahren mittels Videokonferenz durchzuführen.

2) Verantwortlicher

Verantwortlicher für die Verarbeitung personenbezogener Daten im Zusammenhang mit der Online-Mediation ist:
Name, Anschrift / Firma des Mediators

Zusätzlicher Hinweis, falls der Dienstanbieter eine Anwendungssoftware zum Download bereitstellt / das Anlegen eines Benutzerkontos anbietet:
Hinweis: Wenn Sie die Webseite des VK-Anbieters aufrufen, um ein Benutzerkonto anzulegen / die Anwendung für den VK-Dienst herunterzuladen, ist der VK-Anbieter für die Datenverarbeitung in diesem Zusammenhang verantwortlich. Nähere Informationen hierzu finden Sie unter *Einfügen des Links auf die Datenschutzinformationen des VK-Anbieters.* Der VK-Dienst ist jedoch auch über eine Web-Browser-Version nutzbar. Näheres finden Sie in der Einladung.

3) Auftragsverarbeiter

Der Verantwortliche setzt den VK-Anbieter zur Erbringung des VK-Dienstes für die Zwecke der Online-Mediation als Auftragsverarbeiter ein und hat mit ihm dazu eine Auftragsverarbeitungsvereinbarung geschlossen.

4) Übersicht über die Verarbeitungen bei der Online-Mediation

Die folgende Übersicht fasst die Arten der verarbeiteten Daten und die Verarbeitungszwecke sowie die betroffenen Personen zusammen.

Arten der verarbeiteten Daten
Die folgenden Datenarten werden im Zusammenhang mit der Durchführung der Videokonferenz verarbeitet:

- Vorname, Nachname, E-Mail-Adresse der Teilnehmer
- Teilnehmer-IP-Adressen, Geräte-/Hardware-Informationen, Einwahlzeitpunkt
- Textdatei des Chats, soweit der Chat verwendet wird
- Audio- und Videodaten der Videokonferenz: Zur Ermöglichung der Videokonferenz (Bild- und Audioübertragung) werden während der Dauer der Online-Mediation die Daten von Mikrofon und Kamera Ihres Endgeräts verarbeitet. Mikrofon und Kamera können jederzeit von Ihnen aus- und wieder eingeschaltet werden.

Umfang und Zweck der Datenverarbeitung
Die Datenverarbeitung erfolgt im folgenden Umfang und zu den folgenden Zwecken:

- Der VK-Dienst wird verwendet, um die Online-Mediation durchzuführen. Eine Aufzeichnung findet nicht statt. Die personenbezogenen Daten werden grundsätzlich nur während der Dauer der jeweiligen Sitzung der Online-Mediation verarbeitet.
- Soweit am geteilten Bildschirm Visualisierungen zur Unterstützung der Online-Mediation erfolgen, können diese mit Einwilligung aller Teilnehmer vom Mediator gespeichert und in späteren Sitzungen wieder verwendet werden. Mit Einwilligung aller Teilnehmer ist ebenfalls eine Überlassung an die Teilnehmer möglich.

- Der Chat wird ggf. für die Mitteilung von Informationen während der Sitzung verwendet. Eine Aufzeichnung findet nicht statt. Der Chatinhalt kann mit Einwilligung aller Teilnehmer vom Mediator gespeichert und den Teilnehmern überlassen werden.

Rechtsgrundlage der Datenverarbeitung
Die Datenverarbeitung erfolgt zur Durchführung der Online-Mediation, mithin zur Erfüllung des zwischen Ihnen und dem Verantwortlichen geschlossenen Mediationsvertrages. Die Rechtsgrundlage ist Art. 6 Abs. 1 S. 1 lit. b. DSGVO.

Empfänger / Weitergabe von Daten
Personenbezogene Daten, die im Zusammenhang mit Online-Mediation verarbeitet werden, werden notwendigerweise zur Durchführung der Videokonferenz an den VK-Anbieter weitergegeben und von diesem gemäß dem Auftragsverarbeitungsvertrag verarbeitet.

Zusätzlicher Hinweis, falls der Dienstanbieter eine Anwendungssoftware zum Download bereitstellt / das Anlegen eines Benutzerkontos anbietet: Soweit Sie über ein Benutzerkonto beim VK-Anbieter verfügen und/oder eine Anwendungssoftware zur Teilnahme an der Videokonferenz verwenden, erfolgen zusätzliche Verarbeitungen durch den VK-Anbieter selbst. Weitere Informationen hierzu finden Sie unter *Einfügen des Links auf die Datenschutzinformationen des VK-Anbieters.*

Ort der Datenverarbeitung
Alternative 1: Eine Datenverarbeitung findet nur durch europäische Dienstanbieter innerhalb des Europäischen Wirtschaftsraums statt.
Alternative 2: Eine Datenverarbeitung findet nur durch europäische Dienstanbieter innerhalb des Europäischen Wirtschaftsraums und solcher Länder statt, für die ein Angemessenheitsbeschluss der Europäischen Kommission ein hinreichendes Datenschutzniveau bestätigt hat.
Alternative 3 (derzeit nicht rechtssicher. Kann verwendet werden, sobald hinreichende Klarheit über die Umsetzung der final beschlossenen EDSA-Empfehlungen besteht und die VK-Anbieter diese erfüllen und dokumentieren, und ggf. bereits die neuen Standarddatenschutzklauseln final beschlossen sind und verwendet werden): Eine Datenverarbeitung durch den VK-Anbieter außerhalb des Europäischen Wirtschaftsraums ist durch die Auftragsverarbeitungsvereinbarung gem. Art. 28 DSGVO geregelt. Ein angemessenes Datenschutzniveau wird durch die folgenden Maßnahmen gewährleistet:

- Abschluss der sog. EU Standarddatenschutzklauseln in der Fassung vom *TT.MM.JJJJ.*
- falls vom VK-Anbieter vorgesehen: Ende-zu-Ende-Verschlüsselung
- *falls vom VK-Anbieter vorgesehen:* Die zur Durchführung der Videokonferenz erforderlichen Datenverarbeitungen werden nur in Rechenzentren im Europäischen Wirtschaftsraum vorgenommen.
- *Einfügen weiterer Maßnahmen / Link auf Webseite mit weiteren Maßnahmen, die der VK-Anbieter zum Schutz ergreift.*

Dauer der Datenverarbeitung und Löschung

Bei der Videokonferenz anfallende personenbezogene Inhaltsdaten werden nur während der Dauer der Konferenz gespeichert und verarbeitet. Eine dauerhafte Speicherung findet nicht statt. Eine Aufzeichnung ist unzulässig.

Die übrigen von uns verarbeiteten personenbezogenen Daten werden nach Maßgabe geltenden Rechts gelöscht, sobald kein Erfordernis für eine weitere Speicherung und Verwendung Ihrer sonstigen personenbezogenen Daten aus und im Zusammenhang mit dem Mediationsverfahren mehr besteht.

Sofern die Aufbewahrung und Verwendung personenbezogener Daten für andere, gesetzlich zulässige Zwecke erforderlich sind, wird ihre Verarbeitung auf diese Zwecke beschränkt und im Übrigen gesperrt. Dies gilt z. B. für personenbezogene Daten, die handels- oder steuerrechtlichen Aufbewahrungspflichten unterliegen oder deren Speicherung zur Geltendmachung / Ausübung von rechtlichen Ansprüchen oder zur Verteidigung erforderlich ist. Ihre Löschung kommt erst nach Wegfall der jeweiligen Verarbeitungsgründe in Betracht.

5) Ihre Rechte als Betroffene/r

Im Rahmen des geltenden Datenschutzrechts stehen Ihnen als Betroffene/r folgende Rechte zu. Bitte senden Sie uns Ihre Anfrage schriftlich.

- Sie haben das Recht, von uns jederzeit Auskunft über die Sie betreffenden personenbezogenen Daten zu verlangen.
- Ferner haben Sie bei Fehlern in den Daten das Recht, die Berichtigung der Sie betreffenden personenbezogenen Daten zu verlangen.

- Überdies haben Sie unter den gesetzlichen Voraussetzungen das Recht auf Löschung und / oder auf Einschränkung der Verarbeitung, sowie auf Widerspruch gegen die Verarbeitung.
- Und schließlich haben Sie ein Recht auf Datenübertragbarkeit, d.h. Sie können die Sie betreffende personenbezogenen Daten nach Maßgabe der gesetzlichen Vorgaben in einem gängigen Format erhalten.

6) Beschwerderecht

Wenn Sie der Ansicht sind, dass die Verarbeitung der Sie betreffenden personenbezogenen Daten durch uns gegen die DSGVO verstößt, können Sie sich über die Verarbeitung personenbezogenen Daten durch uns bei der Aufsichtsbehörde für den Datenschutz beschweren. Die für uns zuständige Behörde ist: *Einfügen des Namens und der Anschrift der zuständigen Landesdatenschutzbehörde.*

Anhang 4 – Auftragsverarbeitungsvereinbarungen ausgewählter Anbieter

Alfaview, alfatraining Bildungszentrum GmbH, Vereinbarung zur Auftragsverarbeitung gem. Art. 28 DSGVO
https://alfaview.com/wp-content/uploads/2021/03/AVV_alfaview_Maerz2021.pdf
Stand: März 2021

Microsoft Corp., Microsoft-Onlinedienste, Nachtrag zum Datenschutz
https://www.microsoftvolumelicensing.com/DocumentSearch.aspx?Mode=3&DocumentTypeId=67
Stand: Dezember 2020

sichere-videokonferenz.de (Horizon 44 GmbH), Vertrag über die Auftragsverarbeitung personenbezogener Daten nach EU Datenschutz-Grundverordnung (AV-Vertrag)
https://sichere-videokonferenz.de/pdf/2020_11_sichere-videokonferenz.de_AVV.pdf
Stand: November 2020

Wire Swiss GmbH, Datenverarbeitungszusatz („DVZ“)
https://wire.com/de/legal/#dpa
Stand: 30. Juni 2020

Zoom Video Communications Inc., Global Data Processing Addendum
https://zoom.us/docs/doc/Zoom_GLOBAL_DPA.pdf
Stand: November 2020

Über die Autorin

Dr. Annette Ehrnsperger ist Rechtsanwältin und Mediatorin. Die vorliegende Masterarbeit wurde im Rahmen des Studiums Mediation und Konfliktmanagement an der Europa-Universität Viadrina in Frankfurt (Oder) im 11. Jahrgang (2019–2021) erstellt.
Die Autorin ist seit 2001 im Bereich des IT- und Datenschutzrechts tätig. Nach ihrer Promotion im Internetrecht sammelte sie erste Berufserfahrung als Inhouse-Juristin bei einem der beiden ersten deutschen Internet-Anbieter. Seit 2001 arbeitet sie, inzwischen als Legal Department Sen. Mgr., für ein großes Unternehmen für betriebswirtschaftliche Software im Südwesten Deutschlands. Die Autorin ist zudem Mitglied des konzerninternen Mediator:innenpools. Dort und auch bei der rechtlichen Begleitung komplexer IT-Projekte von den Vertragsverhandlungen bis zum Projektabschluss, sowie im Rahmen ihrer ehrenamtlichen Tätigkeiten, ist sie konfliktbegleitend und lösungsunterstützend tätig.