BUNDESNOTARKAMMER
KÖRPERSCHAFT DES ÖFFENTLICHEN RECHTS

Referentenentwurf eines Gesetzes zur Förderung des Einsatzes von Videokonferenztechnik in der Zivilgerichtsbarkeit und den Fachgerichtsbarkeiten

Stellungnahme der Bundesnotarkammer

13. Januar 2023

Zusammenfassung:

Wir begrüßen das Ziel des vorliegenden Referentenentwurfs, den Einsatz von Videokonferenztechnik in der Zivilgerichtsbarkeit und den Fachgerichtsbarkeiten moderner und zeitgemäßer auszugestalten. In geeigneten Fällen kann die Zuschaltung von Verfahrensbeteiligten mittels einer Bild- und Tonübertragung den Zugang zur Justiz erleichtern, gerichtliche Verfahren beschleunigen und unnötigen Reiseaufwand vermeiden.

Eine zeitgemäße Digitalisierung rechtsstaatlicher Prozesse darf sich jedoch nicht darauf beschränken, die verfahrensrechtlichen Grundlagen zu schaffen, sondern muss immer auch deren technische Umsetzung im Blick haben. Insbesondere datenschutzrechtliche Vorgaben sowie die Identifikation der Verfahrensbeteiligten müssen höchsten Ansprüchen genügen. Dies gilt umso mehr, als es sich bei den erfassten Verfahren um Kernfunktionen staatlicher Hoheitsgewalt handelt.

Wir regen daher an, technische Sicherheitsanforderungen an die zum Einsatz kommenden Videokonferenzsysteme zu normieren. Andernfalls drohen datenschutzrechtliche Anforderungen unterlaufen zu werden. Ferner besteht die Gefahr des Zugriffs privater und fremdstaatlicher Akteure auf sensible rechtsstaatliche Vorgänge (A.).

Auch enthält der Referentenentwurf keine ausdrücklichen Vorgaben zur Identifizierung der per Videokonferenz zugeschalteten Verfahrensbeteiligten durch das Gericht, den Urkundsbeamten der Geschäftsstelle oder den Gerichtsvollzieher, obgleich mit der in sämtlichen gültigen Personalausweisen enthaltenen Online-Funktion (eID) eine zeitgemäße staatliche Infrastruktur mit deutlich höherem Schutzniveau zur Verfügung steht (B.).

Sollte der Gesetzgeber – trotz der aufgeworfenen Bedenken – daran festhalten, keine näheren technischen Anforderungen für die Videokommunikation in der Zivilgerichtsbarkeit und der Fachgerichtsbarkeit festzulegen, darf keinesfalls das hohe Schutzniveau bei der Durchführung notarieller Online-Verfahren unterlaufen werden. Zwischen notariellen Beurkundungsverhandlungen einerseits und den vom Referentenentwurf erfassten Verfahren der Justiz andererseits bestehen deutliche strukturelle wie auch rechtliche Unterschiede. Vor diesem Hintergrund sind jedenfalls im Rahmen notarieller Verfahren höchste Sicherheitsvorkehrungen erforderlich. Diese Unterschiede sollten jedenfalls in der Begründung ausdrücklich Berücksichtigung finden. Andernfalls droht nicht zuletzt eine erhebliche Schwächung des Registerwesens (C.).

Im Einzelnen:

A. Gewährleistung der Vertraulichkeit und Integrität rechtsstaatlicher Prozesse

Der Referentenentwurf sieht vor, dass der Einsatz von Videokonferenztechnik zur Durchführung von mündlichen Verhandlungen (§ 128a ZPO-E) und der Beweisaufnahme (§ 284 Abs. 2

ZPO-E) erweitert und flexibilisiert wird. Auch die Beratung und Abstimmung der Richterinnen und Richter eines Spruchkörpers soll künftig ausdrücklich mittels Bild- und Tonübertragung zulässig sein (§ 193 Abs. 1 GVG-E). Anträge und Erklärungen, die nach § 129a Abs. 1 ZPO vor einem Urkundsbeamten der Geschäftsstelle abzugeben sind, sollen künftig ebenfalls mittels Videokommunikation erfolgen können (§ 129a Abs. 2 ZPO-E). Schließlich wird die Abnahme der Vermögensauskunft durch den Gerichtsvollzieher um die Möglichkeit erweitert, die Auskunft per Bild- und Tonübertragung abzunehmen (§ 802f Abs. 2 Nr. 4 ZPO-E).

Der Referentenentwurf geht dabei grundsätzlich davon aus, dass die Software privater Anbieter zur Anwendung kommt. Er enthält keine Vorgaben über technische Mindestvoraussetzungen und Sicherheitsanforderungen. Es ist damit zu befürchten, dass die Belange des Datenschutzes und der IT-Sicherheit beim Einsatz von Videoübertragungen unterlaufen werden (I.). Die Abwicklung hochsensibler rechtsstaatlicher Prozesse wird den Begehrlichkeiten privater und fremdstaatlicher Akteure ausgeliefert (II.). Die Digitalisierung in der Zivilgerichtsbarkeit und in den Fachgerichtsbarkeiten bliebe hinter etablierten Sicherheitsstandards zurück (III.). Insgesamt erweist sich die Nutzung frei verfügbarer Videokonferenzplattformen privater Anbieter für hoheitliche Verfahren als problematisch (IV.).

I. Fehlen technischer und datenschutzrechtlicher Mindeststandards

Ausweislich der Begründung des Referentenentwurfs sollen die Gerichte bei der Auswahl der verwendeten Videokonferenzsoftware grundsätzlich freie Hand haben. Ausdrücklich zulässig sei auch die Nutzung webbasierter Anwendungen auf den Privatcomputern von Richtern, Urkundsbeamten und Gerichtsvollziehern.[1] Der Entwurf geht damit davon aus, dass grundsätzlich sämtliche auf dem Markt angebotenen Softwarelösungen für die Durchführung von Online-Verhandlungen und -Beweisaufnahmen, für die Abgabe von Prozesserklärungen und für die Abnahme der Vermögensauskunft genutzt werden können. Die Auswahl des Programms steht im Ermessen des Vorsitzenden Richters, des Urkundsbeamten der Geschäftsstelle bzw. des Gerichtsvollziehers. Bestimmte Sicherheitsvorkehrungen, technische Schutzmaßnahmen oder datenschutzrechtliche Mindeststandards werden im Entwurf grundsätzlich nicht vorgeschrieben.[2]

Dies wird der zentralen Bedeutung solcher Verfahren für den Rechtsstaat und der Schutzbedürftigkeit der in diesen Videokonferenzen verhandelten Inhalte nicht gerecht. Mündliche Verhandlungen betreffen sensible personenbezogene Daten – insbesondere im Fall des arbeitsgerichtlichen Verfahrens sind in der Regel sogar besondere Kategorien personenbezogener Daten i.S.d. Art. 9 Abs. 1 DS-GVO betroffen. Häufig werden intime oder

[1] RefE, S. 28.

[2] Für die vom richterlichen Beratungsgeheimnis (§ 43 DRiG) besonders geschützte richterliche Beratung und Abstimmung beschränkt sich § 193 Abs. 1 Satz 2 GVG-E darauf, allgemein anzuordnen, dass durch „organisatorische und technische Maßnahmen die Wahrung des Beratungsgeheimnisses sicherzustellen“ sei. Die Entwurfsbegründung enthält hierzu den abstrakt gehaltenen Hinweis, die Datenübermittlung müsse verschlüsselt erfolgen. Welche Art der Verschlüsselung zur Wahrung des Beratungs- und Abstimmungsgeheimnisses erforderlich ist und wie die Verschlüsselung technisch ausgestaltet sein muss, wird hingegen nicht weiter spezifiziert.

geheimhaltungsbedürftige Sachverhalte erörtert. Endurteile bilden die Grundlage des staatlichen Gewaltmonopols im Rahmen der Zwangsvollstreckung (§ 704 ZPO). Die Vertraulichkeit der richterlichen Beratung und Abstimmung ist unmittelbarer Ausfluss der richterlichen Unabhängigkeit. Ein Verstoß gegen das Beratungs- und Abstimmungsgeheimnis ist nach § 353b Abs. 1 StGB sogar strafbewehrt.[3] Bei der Abnahme einer Vermögensauskunft durch den Gerichtsvollzieher hat der Schuldner vollumfassend Auskunft über alle ihm gehörenden Vermögensgegenstände im In- und Ausland zu geben und ist entsprechend schutzbedürftig. Die Abwicklung dieser Sachverhalte per Videokonferenz muss daher höchsten Anforderungen an Datenschutz und IT-Sicherheit genügen.

Enthält das Gesetz hierzu keine speziellen, konkretisierenden Vorgaben, ergeben sich Datenschutz- und IT-Sicherheitsanforderungen an die für eine Videoübertragung genutzte Technik lediglich aus der unmittelbaren Anwendbarkeit der DS-GVO.[4] Der jeweilige Betreiber einer Videokonferenzsoftware hat zwar gemäß Art. 28 Abs. 3 Satz 2 lit. c DS-GVO anzugeben, welche technischen und organisatorischen Maßnahmen er ergreift. Aufgrund ihrer branchenübergreifenden und technikneutralen Ausgestaltung handelt es sich bei den Vorschriften der DS-GVO aber weitgehend um sehr allgemeine Vorgaben.[5] Ohne besondere technische Fachkenntnisse können Richter, Urkundsbeamte der Geschäftsstelle und Gerichtsvollzieher daher nicht überprüfen und abschließend beurteilen, ob kommerzielle Videokonferenzplattformen eine sichere Datenverarbeitung durch ausreichende technische und organisatorische Maßnahmen gewährleisten oder etwa unzulässige Datenübermittlungen in Drittländer vornehmen.

Dies gilt umso mehr, als Gerichte im Rahmen ihrer justiziellen Tätigkeit nach Art. 55 Abs. 3 DS-GVO keiner datenschutzrechtlichen Aufsicht unterliegen und nach Art. 37 Abs. 1 lit. a DS-GVO im Rahmen ihrer justiziellen Tätigkeit auch keinen Datenschutzbeauftragten zu benennen brauchen.[6]

Ein digitaler Rechtsstaat muss daher auch Vorgaben zur technischen Umsetzung der Videokonferenzverfahren machen. Rechtsstaatliche Standards werden geschwächt, wenn die Auswahl der für geeignet erachteten Software in einer freien Ermessensentscheidung im Einzelfall erfolgt.

II. Gefahr des Abflusses hochsensibler Daten ins Ausland

Fehlen technische und datenschutzrechtliche Mindeststandards besteht die Gefahr, dass hochsensible Daten ins Ausland abfließen. Mit Blick auf die marktübliche Software für

[3] *Staats,* Deutsches Richtergesetz, 2012, § 43 Rn. 11.
[4] RefE, S. 34.
[5] Vgl. Erwägungsgründe 13, 15, 76 DS-GVO; ferner *Flache* in Flache, Praxishandbuch Datenschutz im Notariat, 2021, § 1 Rn. 7 ff.
[6] *Drewes* in Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 37 Rn. 10; *Boehm* in Kühling/Buchner, DS-GVO/BDSG, 3. Aufl. 2020, Art. 55 Rn. 15.

Videokommunikationsdienste dürfte die Übermittlung personenbezogener Daten in Drittländer in vielen Fällen bereits für sich einen Verstoß gegen die Art. 44 ff. DS-GVO darstellen.

Einerseits zeigt die Praxis der gängigen Anbieter, dass sich eine Übermittlung der Daten in einen Drittstaat kaum sicher vermeiden lässt. Zahlreiche marktstarke Anbieter wie Zoom, Google Hangouts und Microsoft Teams wickeln Videokonferenzen über Server ab, die sich in den USA befinden. Selbst Vereinbarungen der Justizverwaltungen mit entsprechenden Anbietern können nicht sicher garantieren, dass es nicht zu entsprechenden Datenabflüssen kommt.[7] Andererseits kann – sofern die Muttergesellschaft des Anbieters in einem Drittland ansässig ist – auch bei einer Datenverarbeitung auf europäischen Servern nicht ausgeschlossen werden, dass Daten in ein Drittland übermittelt werden. Exemplarisch hierfür ist der sog. Cloud-Act.[8] Zwar ist derzeit ein neuer Angemessenheitsbeschluss i.S.d. Art. 45 Abs. 3 Satz 1 DS-GVO geplant. Jedoch sieht sich dieser bereits jetzt starker Kritik ausgesetzt.[9] Das Schutzniveau personenbezogener Daten kann demnach im außereuropäischen Ausland regelmäßig nicht garantiert werden.

Im Fall der Verwendung von Videokonferenzsoftware durch Gerichte, Urkundsbeamte der Geschäftsstelle und Gerichtsvollzieher wird außerdem ein nicht unerheblicher Aspekt staatlicher Souveränität gefährdet. Die Videokonferenzen dienen der Ausübung rechtsstaatlicher Kernfunktionen. Durch gesetzliche Vorgaben muss ausgeschlossen werden, dass diese Ausübung unmittelbar hoheitlichen Handelns auf Servern im Ausland stattfindet und der technische Vollzug von Staatsgewalt der Einflussnahme fremdstaatlicher Akteure, ggf. sogar ihrer Geheimdienste, ausgeliefert wird.

III. Kein Zurückbleiben hinter etablierten Sicherheitsstandards

Insbesondere im Bereich des elektronischen Rechtsverkehrs hat sich die Justiz in den vergangenen Jahren erfolgreich um die Gewährleistung der IT-Sicherheit und Einhaltung der datenschutzrechtlichen Anforderungen bemüht. Hier besteht eine umfassende digitale Infrastruktur, an die die Durchführung gerichtlicher Verfahren anknüpfen kann. Keinesfalls sollten die jahrelangen Bemühungen um einen hohen Sicherheitsstandard im elektronischen Rechtsverkehr durch mangelhaft abgesicherte gerichtliche Videoverfahren konterkariert werden.

Beim elektronischen Rechtsverkehr mit der Gerichtsbarkeit wird auf die sichere Datenübermittlung – angesichts der Sensibilität der übermittelten Daten zu Recht – besonderer Wert gelegt. Als Empfangspostfach der Justiz fungiert dabei ein Elektronisches Gerichts- und Verwaltungspostfach (EGVP). Die Übermittlung erfolgt im Wege der

[7] Siehe hierzu *Schild* in BeckOK Datenschutzrecht, 42. Ed., Stand: 1.11.2022, Syst. E. Datenschutz bei Gerichten und Staatsanwaltschaften, Rn. 55g; auf dieses Risiko weisen auch *Freye*/*Schnebbe*, ZD 2020, 502, 505 hin; zum Schutzniveau in den USA ausführlich EuGH, NJW 2020, 2613, 2619 ff.
[8] *Conrad*/*Licht*/*Strittmatter* in Auer-Reinsdorff/Conrad, Handbuch IT- und Datenschutzrecht, 3. Aufl. 2019, § 22 Rn. 196.
[9] *Haar*, iX 2022, Ausgabe 12, 36.

Ende-zu-Ende-Verschlüsselung.[10] Dadurch ist die Vertraulichkeit des Nachrichteninhalts sichergestellt.[11] Auch das vom Gerichtsvollzieher aufgrund der Vermögensauskunft erstellte Vermögensverzeichnis ist grundsätzlich verschlüsselt an das Vollstreckungsgericht zu übermitteln (§ 4 Abs. 2 Satz 2 VermVV).

Es erscheint daher nicht stimmig, wenn im Rahmen der vom Referentenentwurf erfassten Videoverfahren erheblich niedrigere Sicherheitsanforderungen an die Abgabe prozessualer Erklärungen gestellt werden sollten. Gerade private Videokonferenzplattformen fallen immer wieder durch erhebliche Sicherheitslücken auf[12] und sind Ziel erfolgreicher Hackerangriffe.[13] Die im Vorfeld und im Nachgang der erfassten Verfahren etablierten hohen Sicherheitsstandards werden hierdurch unterlaufen.

IV. Grundlegende Bedenken gegen die Nutzung privater Softwareangebote

Im Ergebnis erweist sich die Nutzung frei verfügbarer Videokonferenzplattformen privater Anbieter für hoheitliche Verfahren generell als problematisch.

Seit dem 1. August 2022 sind in bestimmten Anwendungsbereichen des Gesellschaftsrechts notarielle Online-Verfahren rechtlich zulässig.[14] Das zugrunde liegende Videokommunikationssystem hat die Bundesnotarkammer als Körperschaft des öffentlichen Rechts aufgrund eines gesetzlichen Auftrags (§ 78 Abs. 1 Satz 2 Nr. 10, § 78p Abs. 1 BNotO) entwickelt. Entwicklung und Betrieb erfolgen hoheitlich in Form der mittelbaren Staatsverwaltung.[15] Notarielle Online-Verfahren können einzig über die hoheitlich zur Verfügung gestellte Software durchgeführt werden; die Nutzung anderer Softwareangebote ist untersagt (§ 16a Abs. 1, § 40a Abs. 1 BeurkG). Durch die Nutzung dieses hoheitlichen Videokommunikationssystems für die notarielle Verhandlung wird sichergestellt, dass die digitale Beurkundung ein weitgehendes Funktionsäquivalent zur Präsenzverhandlung bildet. Dadurch wird eine sichere, manipulationsresistente und zuverlässige Beurkundung mittels Videokommunikation gewährleistet.[16]

[10] *Eickelberg*, NZG 2015, 81, 84.

[11] *Kersting/Wettich* in Hoeren/Sieber/Holznagel, Handbuch Multimediarecht, 58. EL, Stand: März 2022, Teil 24 Digitale Justiz Rn. 27; die elektronische Kommunikation mit den Gerichten ist in § 130a ZPO und der Elektronischen Rechtsverkehr Verordnung (ERVV) geregelt, siehe hierzu *von Selle* in BeckOK ZPO, 47. Ed., Stand: 1.12.2022, § 130a Rn. 11 ff. und *Ulrich/Schmieder,* NJW 2019, 113.

[12] Bei dem Anbieter „Zoom" sollen nach Medienberichten Kaufangebote von Zugangsdaten für hunderttausende Accounts im Darknet abgegeben worden seien, vgl. https://www.heise.de/security/meldung/Zugangsdaten-fuer-hunderttausende-Zoom-Accounts-zum-Kauf-im-Darknet-entdeckt-4701838.html; Hinweise auf Sicherheitslücken, vgl. https://www.heise.de/security/meldung/Videokonferenzsoftware-Hacker-verkaufen-angeblich-Exploits-fuer-Zoom-Luecken-4703658.html (alle Artikel zuletzt abgerufen am 13. Januar 2023).

[13] Anhörung von mutmaßlichem Twitter-Hacker gehackt, https://www.berliner-zeitung.de/news/hacker-stoeren-gerichtstermin-mit-mutmasslichem-twitter-hacker-li.97204; Störungen von Onlinekursen: „Zoombombing" an Berliner Unis, https://www.tagesspiegel.de/berlin/zoombombing-an-berliner-unis-4784602.html; Cyberkriminelle entdecken Microsoft Teams als Malware-Schleuder https://www.netzwoche.ch/news/2022-02-21/cyberkriminelle-entdecken-microsoft-teams-als-malware-schleuder (alle Artikel zuletzt abgerufen am 13. Januar 2023).

[14] Gesetz zur Umsetzung der Digitalisierungsrichtlinie (DiRUG) v. 5. Juli 2021, BGBl. I S. 3338 und Gesetz zur Ergänzung der Regelungen zur Umsetzung der Digitalisierungsrichtlinie und zur Änderung weiterer Vorschriften (DiREG) v. 15. Juli 2022, BGBl. I S. 1146.

[15] *Hushahn* in BeckOK BNotO, 6. Ed., Stand: 1.8.2022, § 78p Rn. 2.

[16] RegE DiRUG, BT-Drucks. 19/28177, S. 115 f.; *Bremkamp* in BeckOK BeurkG, 7. Ed., Stand: 15.9.2022, § 16a Rn. 8 f.; *Hushahn* in BeckOK BNotO, 6. Ed., Stand: 1.8.2022, § 78p Rn. 2.

Wünschenswert wäre, dass die Justizverwaltung für die Gerichtsbarkeit ebenfalls ein eigenes, besonders gesichertes Videokommunikationssystem entwickelt und betreibt. Die Entwicklung einer eigenen Videoplattform mag mit einem gewissen Aufwand verbunden sein. Sie stellt jedoch eine zweckmäßige Investition zur Digitalisierung unter gleichzeitiger Förderung von Rechtssicherheit und Rechtsstaatlichkeit dar.

Die Digitalstrategie der Bundesregierung formuliert daher das Ziel, spätestens ab 2024 ein bundeseinheitliches Videoportal der Justiz deutschlandweit für Videoverhandlungen und Online-Termine der Justiz bereitzustellen.[17] Es erscheint vor diesem Hintergrund übereilt, jetzt noch den Einsatzbereich privater Videokommunikationssysteme auszuweiten. Hoheitliche Gerichtsverfahren sind nicht vergleichbar mit privatwirtschaftlichen Geschäftsmeetings.

B. Rechtssichere Identifizierung

Der Referentenentwurf enthält auch keine Vorgaben zur Identifizierung der Beteiligten. Nach der Begründung reiche es aus, wenn ein Ausweisdokument durch Abfilmen sichtbar gemacht werde (sog. Video-Ident-Verfahren).[18] Ein Rückgriff auf elektronische Identitätsnachweise, wie sie etwa in sämtlichen gültigen Personalausweisen enthalten sind (§ 18 PAuswG), findet nicht statt.

Die Beteiligten in den gerichtlichen Verfahren stellen Anträge, machen Aussagen und geben – im Fall der Abnahme einer Vermögensauskunft durch den Gerichtsvollzieher – sogar eidesstattliche Versicherungen ab. Im Interesse der Rechtssicherheit muss die Identität der handelnden Personen daher eindeutig feststehen. Video-Ident-Verfahren sind keinesfalls geeignet, Manipulation und Identitätstäuschung auszuschließen.

Mit der Videoübertragung einhergehende Qualitätseinbußen erlauben keine Kontrolle der Sicherheitsmerkmale eines Ausweisdokuments, die rechtsstaatlichen Ansprüchen an ein hoheitliches Verfahren genügen. Fälschungen können auf diese Weise nicht erkannt werden, zumal eine Inaugenscheinnahme und haptische Überprüfung auf Veränderungen unmöglich sind. Zudem erlauben zahlreiche technische Manipulationsmöglichkeiten die Umgehung einer Identitätsprüfung mittels Video-Ident-Verfahren schon mit einfachen Mitteln. Unlängst wurde etwa das Video-Ident-Verfahren der gematik mithilfe allgemein zugänglicher Open-Source-Software überlistet und eine falsche Identität vorgetäuscht.[19]

Vor diesem Hintergrund stellte der Gesetzgeber an anderer Stelle berechtigt fest, dass Video-Ident-Verfahren und ähnliche, in der Privatwirtschaft heute zum Teil gebräuchliche internetgestützte Identifizierungsverfahren insbesondere vor dem Hintergrund der

[17] Digitalstrategie – Gemeinsam digitale Werte schöpfen, S. 46.
[18] RefE, S. 42.
[19] https://www.ccc.de/de/updates/2022/chaos-computer-club-hackt-video-ident (zuletzt abgerufen am 13. Januar 2023).

Manipulationsanfälligkeit vieler ausländischer Ausweisdokumente fälschungsanfällig sind und damit nicht abschätzbare Sicherheitslücken bergen, die in krimineller Absicht ausgenutzt werden könnten.[20]

Es erscheint naheliegend und mit vergleichsweise geringem Aufwand umsetzbar, die erprobte und allgemein verfügbare Online-Funktion von Ausweisdokumenten (eID) auch für die vom Referentenentwurf erfassten Verfahren fruchtbar zu machen. Die eID-Funktion bildet den zentralen Baustein für die Digitalisierung der öffentlichen Daseinsvorsorge.[21] Sie dient deshalb auch in der Digitalstrategie der Bundesregierung als einheitliches Identifizierungsmittel, mit dem sich Bürgerinnen und Bürger im digitalen Raum gegenüber staatlichen Akteuren ausweisen sollen.[22] Der digitale Zugang zur Justiz unter Verwendung einer eID wird darin ausdrücklich als zukunftsträchtiges Beispiel genannt.[23] Es erscheint widersprüchlich, nun hinter diesem Standard zurückzubleiben.

C. Höheres Schutzniveau der notariellen Online-Verfahren

Zwischen notariellen Beurkundungsverfahren einerseits und gerichtlichen Verfahren, Beweisaufnahmen, richterlichen Beratungen und Abstimmungen und der Abnahme von Vermögensauskünften andererseits bestehen maßgebliche Unterschiede. Diese machen jedenfalls im Rahmen notarieller Verfahren höchste Sicherheitsvorkehrungen erforderlich (I.). Sollte der Gesetzgeber trotz der aufgeworfenen Bedenken unverändert an seinem Vorhaben festhalten, so sollten die jeweils typischen Wesensmerkmale in der Entwurfsbegründung berücksichtigt und entsprechend dargestellt werden (II.).

I. Unterschiede gerichtlicher und notarieller Verfahren

1. Geheimhaltung versus Öffentlichkeitsgrundsatz

Notarielle Verfahren sind nicht öffentlich. Gemäß § 18 Abs. 1 BNotO sind Notarinnen und Notare im Hinblick auf alles, was ihnen bei Ausübung ihres Amtes bekannt geworden ist, umfassend zur Verschwiegenheit verpflichtet. Dieser Verschwiegenheitspflicht unterliegen auch die nach § 26 BNotO zu verpflichtenden Personen, also notarielle Beschäftigte sowie diejenigen Personen, die im Rahmen einer berufsvorbereitenden Tätigkeit oder einer sonstigen Hilfstätigkeit an der Amtstätigkeit mitwirken, sowie ggf. beauftragte Dienstleister nach § 26a BNotO.[24] Hintergrund der Verschwiegenheitspflicht ist, dass Notarinnen und Notare für ihre Amtstätigkeit umfassenden Einblick in die persönlichen und familiären Verhältnisse sowie die Vermögenssituation der Beteiligten benötigen. Sie können ihre hoheitliche Amtstätigkeit im Rahmen der vorsorgenden Rechtspflege daher nur erfüllen, wenn sie Vertrauen genießen.

[20] So RegE DiRUG, BT-Drucks. 19/28177, S. 121.
[21] BT-Drucks. 19/8038, S. 28;
[22] Digitalstrategie – Gemeinsam digitale Werte schöpfen, S. 42 f.
[23] Digitalstrategie – Gemeinsam digitale Werte schöpfen, S. 45 f.
[24] *Sander* in BeckOK BNotO, 6. Ed., Stand: 1.8.2022, § 18 Rn. 19.

Dieses Vertrauen wird ihnen entgegengebracht, weil die Verschwiegenheit über das Anvertraute gewährleistet ist. Die Wahrung der Vertraulichkeit ist somit eine der wichtigsten Amtspflichten und gehört zum Kreis der sog. notariellen „Kardinalpflichten".[25] Die Verschwiegenheitspflicht besteht vorrangig im Interesse der Beteiligten und schützt deren Recht auf informationelle Selbstbestimmung nach Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG.[26] Geschützt wird aber auch das Vertrauen der Allgemeinheit in die Verschwiegenheit der Notarinnen und Notare. Die Geheimhaltung hat damit auch institutionelle Bedeutung.[27] Sie ist die Grundlage notarieller Amtstätigkeit. Die Beteiligten und die Allgemeinheit dürfen darauf vertrauen, dass notarielle Verfahren dem Zugriff der Öffentlichkeit entzogen sind. Dieses Vertrauen würde erheblich erschüttert, wenn aufgrund einer unsicheren Videokonferenzplattform Aufzeichnungen notarieller Verfahren an die Öffentlichkeit gelangen würden.

Demgegenüber gilt für gerichtliche Verfahren – mit Ausnahme von Beratungen und Abstimmungen nach § 193 GVG – der Öffentlichkeitsgrundsatz. Gemäß § 169 Abs. 1 Satz 1 GVG ist die Verhandlung vor dem erkennenden Gericht einschließlich der Verkündung der Urteile und Beschlüsse öffentlich. Verwirklicht sich das Risiko eines Datenzugriffs Dritter, dürften sich die Folgen in der Regel nicht als vergleichbar fatal erweisen, da vom Inhalt der gerichtlichen Verhandlung grundsätzlich bereits kraft Gesetzes Kenntnis genommen werden darf. Ein Eingriff in das Recht auf informationelle Selbstbestimmung wöge weniger schwer. Im Hinblick auf diese gerichtlichen Tätigkeiten gilt keine umfassende Verschwiegenheitspflicht.

Selbstverständlich kann das Vertraulichkeitsniveau aber nur insoweit niedriger bewertet werden, als der Grundsatz der Öffentlichkeit reicht. Das Gesetz räumt dem Vertrauen der Allgemeinheit und der Beteiligten auf Geheimhaltung in bestimmten Bereichen bewusst Vorrang ein. So finden Verhandlungen bei Vorliegen besonderer Gründe zum Schutz der Beteiligten etwa ausnahmsweise unter Ausschluss der Öffentlichkeit statt (§§ 170 ff. GVG).[28] Die richterliche Beratung und Abstimmung ist als reiner Binnenakt des Spruchkörpers ebenfalls nicht öffentlich, um unbefangene Entscheidungen zu ermöglichen. Auch die Abgabe der Vermögensauskunft des Schuldners erfolgt – vom Anwesenheitsrecht des Gläubigers abgesehen – nicht öffentlich.[29] In diesen Situationen dürfte unter dem Aspekt der Verschwiegenheit das Schutzbedürfnis mit dem notarieller Beurkundungsverhandlungen vergleichbar sein.

2. Unterschiedliche Rechtsscheinwirkungen

Erklärungen der Beteiligten, die vor der Notarin bzw. dem Notar abgegeben werden, erzeugen in vielen Fällen Rechtsscheinwirkung. Beispielsweise führen Erklärungen, die im Rahmen eines notariellen Online-Verfahrens abgegeben werden, zu Eintragungen im Handels-, Genossenschafts- und Partnerschaftsregister. Diese Eintragungen entfalten gemäß § 15 HGB, § 29 GenG

[25] *Bremkamp* in Frenz/Miermeister, BNotO, 5. Aufl. 2020, § 18 Rn. 1.
[26] *Püls* in Beck´sches Notar-Handbuch, 7. Aufl. 2019, § 34 Rn. 3.
[27] BGH, DNotZ 2005, 288, 292; *Sander* in BeckOK BNotO, 6. Ed., Stand: 1.8.2022, § 18 Rn. 4.
[28] Zu den Ausschlussgründen in § 172 GVG, siehe *Allgayer* in BeckOK GVG, 16. Ed., Stand: 15.8.2022, § 172 Rn. 1 ff.
[29] *Fleck* in BeckOK ZPO, 47. Ed., Stand: 1.12.2022, § 802c Rn. 9.

und § 5 Abs. 2 PartGG Publizitätswirkung. Der Rechtsverkehr darf und soll gerade auf die Eintragungen im Handelsregister vertrauen. Die Garantie eines verlässlichen Registerinhalts, der die Grundlage des Rechts- und Geschäftsverkehrs bildet, ist damit Kernaufgabe notarieller Formvorschriften. Die weitreichende – die betroffenen Gesellschaften bindende – Publizitätswirkung der Justizregister kann schon verfassungsrechtlich nur gerechtfertigt werden, wenn besondere Schutzvorkehrungen gegen Eintragungen durch Nichtberechtigte getroffen werden.[30] Vor diesem Hintergrund müssen im notariellen Verfahren höchste Anforderungen an die Identitäts- und Authentizitätsprüfung der Beteiligten gestellt werden. Bereits im Präsenzverfahren trifft daher § 10 BeurkG strengere Vorgaben zur Identifizierung, als dies in den vom Referentenentwurf erfassten Verfahren der Fall ist. Aufgrund der zusätzlichen Schwierigkeiten der Identifizierung einer Person in Videokonferenzen werden diese Anforderungen für die notariellen Online-Verfahren in § 16c BeurkG weiter konkretisiert und verschärft. Damit die Publizitätswirkung auch durch Eintragungen gerechtfertigt werden kann, denen ein Online-Verfahren vorausgeht, muss der Notar sich in der Regel in einem zweistufigen Identifizierungsverfahren Gewissheit über die Person der Beteiligten verschaffen.

Erklärungen gegenüber dem Gericht erzeugen dagegen keinen materiellrechtlichen Rechtsschein. Prozesserklärungen gegenüber der virtuellen Antragstelle, die von einer unberechtigten Person abgegeben werden, sind schlicht unwirksam. Auch eine Vermögensauskunft, die gegenüber dem Gerichtsvollzieher im Rahmen einer Videoübertragung abgegeben wird, führt nicht zu einem Rechtsschein mit der materiellrechtlichen Wirkung, dass der Schuldner als Inhaber der beauskunfteten Vermögensgegenstände gelten würde.

3. Ungleiche Missbrauchsanfälligkeit

Die weitreichenden Folgen einer notariellen Beurkundung machen ein missbräuchliches Verhalten durch Identitätstäuschungen ungleich attraktiver, als dies bei den vom Referentenentwurf erfassten Verfahren der Fall ist.

Eine erfolgreiche Täuschung im notariellen Verfahren bewirkt eine positive Registerpublizität. Diese kann zu einer nachhaltigen Erschleichung fremder Vermögenswerte führen. Hingegen dürfte insbesondere im Verfahren zur Abgabe einer Vermögensauskunft selten ein Anreiz bestehen, verdeckt für einen anderen eine Vermögensauskunft abzugeben.

4. Geldwäschebekämpfung

Die rechtssichere Identifizierung der Beteiligten nimmt in den notariellen Verfahren auch zum Zwecke der Geldwäsche- und Terrorismusbekämpfung einen höheren Stellenwert ein, als das in den vom Entwurf erfassten Verfahren der Fall ist:

[30] Vgl. hierzu *Bormann/König*, notar 2008, 256, 259 f.

Notarinnen und Notare werden zur wirksamen Verhütung von Straftaten herangezogen, insbesondere im Bereich von Geldwäsche, Terrorismusfinanzierung, Steuerhinterziehung, Insolvenz- und sonstigen Wirtschaftsstraftaten. Sie sind Verpflichtete nach den geldwäscherechtlichen Vorschriften und unterliegen insoweit spezifischen, besonders strengen Vorgaben zur Identifizierung, § 10 Abs. 1 Nr. 1 sowie §§ 11, 12 des GwG. Eine verlässliche Identifizierung der Beteiligten durch Notarinnen und Notare ist daher unabdingbar, um Schäden für die Beteiligten und die Allgemeinheit zu vermeiden.[31] Dieser Aspekt der Identifizierung spielt bei einer gerichtlichen Videoverhandlung, beim Stellen prozessualer Anträge oder bei der Abgabe einer Vermögensauskunft keine Rolle. Gerichte unterliegen in diesem Bereich ihrer Tätigkeit keinerlei Verpflichtungen nach dem Geldwäschegesetz (§ 2 Abs. 3 GwG).

II. Klarstellung in der Entwurfsbegründung

Der Referentenentwurf bezweckt eine Digitalisierung elementarer justizieller und damit rechtsstaatlicher Prozesse. Vor diesem Hintergrund sprechen wir uns nachdrücklich dafür aus, dem durch höchste Sicherheitsstandards bei der Umsetzung gerecht zu werden. Dies gilt insbesondere für die Fälle, in denen der Öffentlichkeit aus besonderen Gründen eine Teilnahme am gerichtlichen Verfahren versagt ist. Digitalisierung und (Rechts-)Sicherheit sollten stets Hand in Hand gehen. Dass dies technisch umsetzbar ist, belegen die notariellen Online-Verfahren.

Angesichts bestehender Unterschiede zwischen notariellen und gerichtlichen Verfahren ist es sicherlich denkbar, hinsichtlich des Schutzniveaus nicht völlig identische Maßstäbe anzulegen. In Grenzen entspricht dies auch dem risikobasierten Ansatz der DS-GVO. Diese Unterschiede und die verschiedenen daraus folgenden Schutzbedürfnisse sollten in der Begründung des Regierungsentwurfs allerdings klar benannt werden. Andernfalls droht das hohe Schutzniveau notarieller Online-Verfahren langfristig verwässert oder schlimmstenfalls unterlaufen zu werden.

* * *

[31] RegE DiRUG, BT-Drucks. 19/28177, S. 120.

Kontakt:

Bundesnotarkammer K.d.ö.R.

Mohrenstraße 34
10117 Berlin

Telefon: +49 30 383866 – 0
Telefax: +49 30 383866 – 66
E-Mail: bnotk@bnotk.de

Büro Brüssel:
Avenue de Cortenbergh 172
B-1000 Bruxelles

Telefon: +32 2 7379000
Telefax: +32 2 7379009
E-Mail: buero.bruessel@bnotk.de