Bundessteuerberaterkammer, KdöR, Postfach 02 88 55, 10131 Berlin

Bundessteuerberaterkammer
KÖRPERSCHAFT DES ÖFFENTLICHEN RECHTS

Bundesministerium der Justiz
Herrn Dr. Philip Scholz
Referat DB3
Mohrenstr. 37
10117 Berlin

Abt. Steuerrecht und Rechnungslegung

Unser Zeichen: Gs/Gr
Tel.: +49 30 240087-68
Fax: +49 30 240087-77
E-Mail: steuerrecht@bstbk.de

E-Mail: db3@bmj.bund.de
scholz-ph@bmj.bund.de

12. Januar 2023

Stellungnahme zu dem Entwurf eines Gesetzes zur Förderung des Einsatzes von Videokonferenztechnik in der Zivilgerichtsbarkeit und den Fachgerichtsbarkeiten

Sehr geehrter Herr Dr. Scholz,

für die Übersendung des Gesetzentwurfs und die Möglichkeit zur Stellungnahme bedanken wir uns.

I. Vorbemerkung

Aus Sicht der BStBK sind die in dem Entwurf vorgesehenen Anpassungen der zivilprozessualen Grundlagen für den Einsatz von Videokonferenztechnik zu begrüßen. Sie ermöglichen insbesondere eine flexible, ressourcenschonende und im internationalen Vergleich überfällige Nutzung von Videoverhandlungen (§ 128a ZPO-E) und Videobeweisaufnahmen (§ 284 Abs. 2 ZPO-E) in der deutschen Zivil- und Fachgerichtsbarkeit. Der verstärkte Einsatz von Videokonferenztechnik kann zu einer effizienteren Verfahrensführung beitragen, Verfahren beschleunigen und damit das Bild einer modernen und bürgernahen Justiz fördern.

Für die praktische Umsetzung sind u. E. jedoch noch erhebliche Investitionen in die digitale und technische Infrastruktur der Gerichte erforderlich. Derzeit fehlt es der deutschen Justiz an Grundlegendem, um einen bundeseinheitlichen Standard für Videokonferenztechnik gewährleisten zu können. Häufig sind – entgegen der Feststellungen auf Seite 28 des Entwurfs – weder ausreichende Internetbandbreiten, leistungsstarke und moderne Hardware in Form von PC‘s, Kameras und Mikrophonen noch datensichere Softwareanwendungen vorhanden. Damit Videoverhandlungen bzw. hybride Verhandlungen die gleiche Qualität wie Präsenzverhandlungen gewährleisten können, müssen die Gerichte daher zunächst flächendeckend mit verlässlicher Hard- und Software ausgestattet werden.

Um bundesweit einheitliche Standards zu gewährleisten, sollten zudem die Anforderungen an die Videokonferenztechnik klar definiert werden. Die Systeme müssen nutzerfreundlich und praktikabel sein sowie höchsten IT-Sicherheits- und Datenschutzstandards genügen. Es bedarf zudem einer Schulung des Gerichtspersonals und IT-technischer Unterstützung durch die Justizverwaltungen.

Parteianträge auf Videoverhandlungen werden derzeit von den Gerichten oftmals ohne Angabe von Gründen abgelehnt. Insoweit ist es positiv zu bewerten, dass der Entwurf neben einem weiten Gestaltungsspielraum für das Gericht bzw. den Vorsitzenden auch eine Stärkung der Stellung der Prozessparteien in Bezug auf Videoverhandlungen in § 128a Abs. 2 und 3 ZPO-E vorsieht. Insbesondere soll gegen einen ablehnenden Beschluss des Gerichts mittels der sofortigen Beschwerde eine Anfechtungsmöglichkeit implementiert werden. Aus Sicht der BStBK wäre eine weitergehende Regelung, die einen prozessrechtlichen Anspruch verankert, jedoch wünschenswert.

Wir begrüßen es ausdrücklich, dass der Entwurf sowohl hybride als auch rein virtuelle Verhandlungen vorsieht und damit dem Gericht künftig auch Verhandlungen von einem anderen Ort als dem Gerichtssaal aus ermöglicht. Für die Wahrung der Öffentlichkeit gem. § 169 Abs. 1 Satz 1 GVG im Rahmen von vollvirtuellen Verhandlungen sollte u. E. jedoch eine zeitgemäßere Lösung gefunden werden als die mündliche Verhandlung an einen anderen öffentlich zugänglichen Raum im Gericht zu übertragen.

II. Anmerkungen im Einzelnen

Die in dem Entwurf vorgesehenen gesetzlichen Rahmenbedingungen für den Einsatz von Videokonferenztechnik sind weitestgehend zu begrüßen. Damit praktisch von den Regelungen Gebrauch gemacht werden kann, bedarf es jedoch dringend der Implementierung der erforderlichen technischen Ausstattung in den Gerichten und der Präzisierung der datenschutzrechtlichen Aspekte. Unsere diesbezüglichen Hinweise lauten wie folgt:

1. Allgemeine Anforderungen an die Videokonferenztechnik

Aus Sicht der BStBK bedarf es einer Definition der Anforderungen an die Videokonferenztechnik, die höchsten Ansprüchen gerecht werden muss. Die flüssige Übertragung von hochauflösenden Videosequenzen erfordert den Down- und Upstream von großen Datenmengen, die mit den derzeit in der Justiz vorhandenen Internetanschlüssen nicht flächendeckend bewältigt werden können. Die Internetkapazitäten- bzw. Bandbreiten sind dementsprechend aufzurüsten.

Damit es allen Prozessbeteiligten möglich ist, den jeweils Sprechenden zu sehen und diesem folgen zu können, sollte zudem grundsätzlich die Installation von mehreren (ggf. per Einstellung manuell oder automatisiert wechselbaren) Kameras erfolgen. In der derzeitigen Videoverhandlungsführung wird aus dem Berufsstand vielfach bemängelt, dass die anwesenden Prozessparteien bzw. deren Bevollmächtigte meist nur von der Seite und am Bildrand zu sehen sind. Erforderlich sind u. E. daher professionelle Kamerasysteme, die aus verschiedenen Winkeln in hochauflösender Bildqualität aufnehmen oder übertragen können. Gleiches gilt für die Ausstattung mit Mikrophonen.

Den Beteiligten und der Sitzungsleitung sollte das Teilen des jeweils genutzten Bildschirms sowie das Einspielen von Videos und Ton (etwa zur Beweiserhebung und -führung i. S. d. § 284 Abs. 2 ZPO-E) ermöglicht werden. Wichtig ist, dass das Gerichtspersonal entsprechend

technisch geschult wird, damit ein möglichst reibungsloser Ablauf in der jeweiligen Verhandlung gewährleistet ist und alle Beweiserhebungsmöglichkeiten gleich einer regulären Präsenzverhandlung ausgeschöpft werden können. Insoweit gebietet es der fair-trial-Grundsatz, dass die Prozess- und Verfahrensbeteiligten alle ihnen durch das jeweilige Prozessrecht gegebenen Möglichkeiten auch im Rahmen einer Videoverhandlung wahrnehmen können.

Die Einrichtung sog. Breakout-Rooms ermöglicht es der Sitzungsleitung, die verschiedenen Anwesenden ggf. zu separieren und zwischenzeitlich des Raumes zu verweisen. Denkbar ist dies etwa bei Zeugen oder Sachverständigen, die (zunächst) von der Hauptverhandlung/mündlichen Verhandlung getrennt und erst später nach etwaiger Belehrung vernommen werden sollen. Es muss bei der Nutzung der Breakout-Rooms unbedingt technisch sichergestellt werden, dass Zeugen oder Sachverständige keine Möglichkeit haben, sich vor Aufruf durch die Sitzungsleitung in den virtuellen Gerichtssaal einzuwählen.

Das Videokonferenzsystem sollte eine „Meldefunktion“ für Anmerkungen bei Redebedarf beinhalten. Dies ist derzeit bereits in einigen Softwareanwendungen in Form der Betätigung eines Hand-Symbols möglich. Die Sitzungsleitung kann dann dem jeweiligen Teilnehmer das Wort erteilen. Ungebetene Zwischenrufe oder Störungen können so bereits vorweg ausgeschlossen werden, weil das Sprechen stets die entsprechende Worterteilung voraussetzt.

Wichtig ist u. E. die Implementierung von Zulassungskontrollen. Die Einwahl sollte nur mit einer im Programm hinterlegten Mailadresse und einem vorher vergebenen Passwort möglich sein. So kann der Gefahr einer nicht autorisierten Nutzung effektiv begegnet werden. Darüber hinaus muss die Möglichkeit der Identitätskontrolle bei datenschutzrechtlich relevanten Gesprächen durch die Sitzungsleitung bestehen (z. B. über einen digitalen Personalausweis oder ein anderes entsprechendes Legitimationsmedium). Es muss dabei ausgeschlossen werden können, dass eine Zuschaltung ausschließlich per Telefon bzw. Ton durch unbekannte Personen erfolgt.

Der Nutzer muss sich schnell in dem angebotenen Videokonferenztool zurechtfinden und dieses stabil und unterbrechungsfrei nutzen können. Ebenso sollte keine zusätzliche Software installiert werden müssen, die Videokonferenz vielmehr aus dem Browser heraus ausgeführt werden können. Eine Nutzung sollte zudem auch über mobile Geräte, wie Smartphones bzw. Tablets, erfolgen können.

Neben dem Komfort der Nutzung ist aufgrund der Vielzahl von Anwendungen von Bedeutung, dass das verwendete Videokonferenztool interoperabel ist. Dies bedeutet, dass eine Verknüpfung mit anderen im Kontext verwendeten Lösungen gegeben sein muss. Hierzu gehört etwa eine Verknüpfung von Terminkalender und Videokonferenzsystem dahingehend, dass mit einer Terminvereinbarung unmittelbar der notwendige Link übermittelt werden kann. Auch die Möglichkeit, über die Software Dokumente und Links zu teilen oder in gemeinsamen Dokumenten zu arbeiten, erhöht den Nutzen.

2. Datenschutzrechtliche Aspekte

Die Justiz muss bei der Schaffung eines bundeseinheitlichen Standards ein Datenschutzniveau gewährleisten, das höchsten Anforderungen genügt. Auf Seite 34 der Gesetzesbegründung wird diesbezüglich lediglich ausgeführt, dass sich die Datenschutz- und Datensicherheitsanforderungen an die für eine Videoverhandlung genutzte Technik unmittelbar aus Art. 24, 25 und 32 DSVGO ergeben. Unseres Erachtens sollten hier weitere Konkretisierungen erfolgen.

Die Justiz als auch der jeweilige Betreiber der Videokonferenzsoftware müssen klare und eindeutige Informationen über die mit der Nutzung des Dienstes verbundene Datenverarbeitung zur Verfügung stellen. Den Nutzern muss vollumfänglich klar sein, welche Daten für welche Zwecke verarbeitet werden, bzw. wo die Verarbeitung stattfindet und wie lange die Daten gespeichert werden. Außerdem muss der Betreiber darüber informieren, ob und ggf. welche externen Dienstleister (Auftragsverarbeiter i. S. v. Art. 28 DSGVO) er selbst nutzt und an welche anderen Stellen Daten weitergegeben werden. Hierbei ist es wichtig, dass bei Anbietern mit Sitz außerhalb der EU die Anwendung von Standardvertragsklauseln zum Tragen kommt.

Die Verbindungsdaten der Kommunikation (z. B. Kommunikationsteilnehmer, Zeitpunkt, Geräte- und Standortdaten) dürfen nur solange und soweit verarbeitet werden, wie es für die Übermittlung von Nachrichten durch einen Dienstleister oder im Rahmen einer notwendigen Dokumentation erforderlich ist. Bestenfalls sind Dienste zu bevorzugen, die es ermöglichen, die Verarbeitung personenbezogener Daten einzuschränken oder gar ganz auszuschließen. Hier ist kritisch zu hinterfragen, welche Datenverarbeitung für die jeweiligen Dienste tatsächlich überhaupt erforderlich ist und diese auf ein mögliches Minimum zu reduzieren. Im Falle einer Datenübermittlung in sog. Drittländer (d. h. außerhalb des Geltungsbereichs der DSGVO) muss die Übermittlung durch geeignete Garantien gesichert sein.

Auch der Betreiber des Videokonferenzdienstes muss eine hohe Datensicherheit gewährleisten. Diese kann durch eine sichere Nutzer-Authentifizierung und Verschlüsselung der Kommunikationskanäle sowohl bei der Vermittlung der Verbindungen als auch bei der Übertragung von Ton- und Bilddaten (idealerweise über eine Ende-zu-Ende-Verschlüsselung) erreicht werden. Je nach Sensibilität der Daten sollten die eingesetzten Endgeräte über einen wirksamen Zugriffschutz verfügen (z. B. PIN-Schutz oder biometrische Lösungen). Der interne Speicher der Geräte sollte durch Verschlüsselung so geschützt werden, dass eine Entschlüsselung die Kenntnis der Anmeldedaten voraussetzt.

Es ist über die konkrete Regelung des § 128a Abs. 6 Satz 3 ZPO-E hinaus unbedingt sicherzustellen, dass bei den eingesetzten Videokonferenzsystemen das Risiko eines unbefugten Mithörens oder Mitschneidens durch Dritte oder Konferenzteilnehmer selbst ausgeschlossen ist. Auch etwaige behördliche Aufzeichnungspflichten des Betreibers rechtfertigen keinesfalls Mitschnitte und sind daher zu unterbinden. Um einen Mitschnitt des Betreibers von vornherein gänzlich auszuschließen, sollte daher auf die o. g. Ende-zu-Ende-Verschlüsselung zurückgegriffen werden. Diese Regeln gelten umso mehr für nichtöffentliche Verhandlungen. Es ist unbedingt sicherzustellen, dass die Verhandlung im Videoformat nicht zur Aushöhlung der Persönlichkeitsrechte des Einzelnen führt.

Der Sitzungsleitung müssen weitreichende Eingriffsmöglichkeiten zur Verfügung stehen. Der Videokonferenzdienst muss es daher ermöglichen, sowohl Inhaltsdaten (Chat-Transkripte, Audio- und Videoaufzeichnungen, geteilte Dateien oder Screenshots usw.), Metadaten (Teilnehmer eines Meetings oder einer Session) als auch Bestandsdaten (Benutzerkennungen, Namen, Kontaktinformationen usw.) gezielt oder allgemein zu löschen. Er sollte zudem über die Möglichkeit verfügen, eine Frist festzulegen, nach der solche Daten automatisiert gelöscht werden.

Es ist ferner sicherzustellen, dass die Bildung von Benutzerprofilen durch den Videokonferenzdienst bzw. deren Auswertung oder anderweitige Nutzbarmachung (durch den Anbieter bzw. Dritte) gänzlich ausgeschlossen ist.

Auch der sog. Datenschutz im weiteren Sinne sollte bei der Ausarbeitung des Konzepts berücksichtigt werden. Darunter sind solche Maßnahmen zu verstehen, die dazu geeignet sind sicherzustellen, dass Nutzer durch ihr Verhalten nicht gegen bestehende Regelungen verstoßen. Diese Überlegungen basieren auf dem Konzept des „desire path“ nachdem sich Anwender stets den für sie bequemsten Weg aussuchen, selbst wenn dieser Risiken birgt. Die Neigung, Risiken aus Bequemlichkeit einzugehen, ist gerade bei Softwareanwendungen besonders ausgeprägt. Die Nutzerfreundlichkeit darf insoweit nicht zu einem Verlust an Sicherheit führen.

Für Rückfragen stehen wir Ihnen gern zur Verfügung.

Mit freundlichen Grüßen

Claudia Kalina-Kerschbaum
Geschäftsführerin

i. A. Oliver Glückselig
Referatsleiter