Bundessteuerberaterkammer, KdöR, Postfach 02 88 55, 10131 Berlin

Bundesministerium der Justiz und für
Verbraucherschutz
Herrn Malte Büttner
Referat Z C 2
Mohrenstraße 37
10117 Berlin

E-Mail: buettner-ma@bmjv.bund.de

Bundessteuerberaterkammer
KÖRPERSCHAFT DES ÖFFENTLICHEN RECHTS

Abt. Steuerrecht und Rechnungslegung

Unser Zeichen: Hm/Gr
Tel.: +49 30 240087-74
Fax: +49 30 240087-77
E-Mail: steuerrecht@bstbk.de

15. April 2021

Erarbeitung eines Fachkonzepts zur Errichtung eines bundesweiten Standards für Videoverhandlungen

Sehr geehrter Herr Büttner,

wir bedanken uns für die Möglichkeit, zu dem BMJV-Projekt „Bundesweiter Standard für Videoverhandlungen“ wichtige Anregungen aus Sicht des Berufsstandes der Steuerberater geben zu können.

I. Vorbemerkung

Die Implementierung der bereits seit geraumer Zeit gegebenen technologischen Möglichkeiten in die tradierte Prozess- und Verfahrensführung vor deutschen Gerichten ist gerade auch im Hinblick auf einen internationalen Vergleich überfällig und daher ausdrücklich zu begrüßen. Die Corona-Pandemie hat aufgezeigt, dass eine zukunftsfähige Gesellschaft auf die Anwendung moderner Technologien dringend angewiesen ist. Derzeit fehlt es dem Vernehmen nach in der deutschen Justiz jedoch noch an Grundlegendem. Häufig sind weder ausreichende Internetbandbreiten, leistungsstarke und moderne Hardware in Form von PC‘s, Kameras und Mikrophonen noch datensichere Softwareanwendungen vorhanden.

Der nunmehr vorhandene „Digitalisierungsschub“ sollte daher genutzt werden, um die vielerorts zum Standard gewordene Abhaltung von Videokonferenzen auch für die deutsche Justiz einzuführen. Die Erarbeitung bundeseinheitlicher Standards ist sinnvoll und sollte unter Einbezug sämtlicher (potentieller) Nutzergruppen erfolgen. Gerade im Hinblick auf eine Entbürokratisierung sowie die weitere Vereinfachung und Entlastung von Gerichten, Verwaltungen und anderen Prozess- und Verfahrensbeteiligten muss langfristig das volle Potential der modernen Technologien und digitalen Anwendungen ausgeschöpft und effektiv genutzt werden.

Damit verfassungsrechtlich verankerte Prinzipien wie die Ansprüche auf den gesetzlichen Richter sowie den effektiven Rechtsschutz nach den Art. 101 I 2, 19 IV GG gewährleistet sind, ist es unabdingbar, allen Beteiligten eine sichere, einheitliche und verlässliche Plattform zu bieten. Etwaige Hürden wie das föderale System dürfen für die jeweiligen (Rechts-)Anwender und betroffenen Beteiligten/Parteien nicht dazu führen, dass es zu regionalen bzw. qualitativen Unterschieden in der Prozess- und Verfahrensführung kommt. Insoweit sollte ein

bundeseinheitlicher Standard klar definiert werden. Ein lückenloses IT-Sicherheits- und Datenschutzkonzept ist zu gewährleisten.

Es sollte zudem die Verankerung eines prozessrechtlichen Anspruchs auf Verhandlung in Form einer Videokonferenz in Erwägung gezogen werden. Derzeit wird aus der Praxis berichtet, dass trotz der Auswirkungen der Corona-Pandemie den Anträgen von Prozess- und Verfahrensbevollmächtigten auf Durchführung einer Videoverhandlung oft nicht entsprochen wird. Gegen den ablehnenden Beschluss des Gerichts besteht nach geltendem Prozessrecht keine Anfechtungsmöglichkeit. Es würde den Zweck einer flächendeckenden Modernisierung der Justiz konterkarieren, wenn die regelmäßige Durchführung von Videoverhandlungen an der Gunst des jeweiligen Gerichts oder der Präferenz für oder gegen technische Neuansätze scheitern würde. Zudem sollten auch hybride Formate zur Verfügung gestellt werden, sofern nicht alle Beteiligten ihr Einverständnis zu einer Videoverhandlung erteilen. In diesem Fall können die Beteiligten dann teilweise in Persona im Gerichtssaal und teilweise per Videoschaltung teilnehmen.

II. Anregungen im Einzelnen

1. Wichtige Anwendungsgesichtspunkte

Die Gerichte müssen mit ausreichenden Internetkapazitäten- bzw. Bandbreiten ausgestattet werden. Die flüssige Übertragung von hochauflösenden Videosequenzen erfordert den Down- und Upstream von großen Datenmengen, die mit den derzeit in der Justiz vorhandenen Internetanschlüssen nicht bewältigt werden können (vgl. exemplarisch https://www.drb-berlin.de/fileadmin/Landesverband_Berlin/Dokumente/leitfaden_videoverhandlung/Leitfaden_Videoverhandlung__Mai_2020_.pdf, S. 2).

Eine ordentliche technische Infrastruktur der Gerichte ist für die Umsetzung eines einheitlichen Videokonferenzsystems unerlässlich. Damit Videoverhandlungen die gleiche Qualität wie Präsenzverhandlungen gewährleisten können, müssen die Gerichte mit verlässlichen und modernen Computern, Mikrophonen und Kameras ausgestattet werden.

Damit es allen Prozessbeteiligten möglich ist, die jeweils Sprechenden zu sehen und diesen folgen zu können, sollte zudem die Installation von mehreren (ggf. per Einstellung manuell oder automatisiert wechselbaren) Kameras angedacht werden. 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 Kamerasysteme, die aus verschiedenen Winkeln in hochauflösender Bildqualität aufnehmen oder übertragen können.

Den Beteiligten und der Sitzungsleitung sollte das Teilen des jeweils genutzten Bildschirms sowie das Einspielen von Videos und Ton (etwa zur Beweiserhebung- und führung) 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 (Zeuge, Inaugenscheinnahme, Sachverständige etc.)

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.

Zudem erscheint die Einrichtung eines sog. Datenraums sinnvoll, in dem die Anwesenden Dokumente (beispielsweise im PDF-Format) per „Drag and Drop“ zur Gerichtsakte reichen können. Damit hierdurch keine etwaige Schadsoftware auf die Gerichtscomputer gelangt, müsste eine Virenprüfung erfolgen, ehe die Datei abgerufen wird.

Es sollten ferner sog. Breakout-Rooms eingerichtet werden. Dadurch wird es der Sitzungsleitung ermöglicht, 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.

Es sollten ferner Zulassungskontrollen derart durchgeführt werden, dass die Einwahl nur mit einer im Programm hinterlegten Mailadresse und einem vorher vergebenen Passwort möglich ist. So kann der Gefahr einer illegalen Doppelnutzung effektiv begegnet werden. Darüber hinaus muss die Möglichkeit der Identitätskontrolle bei datenschutzrechtlich relevanten Gesprächen (z. B. über einen digitalen Personalausweis oder ein anderes entsprechendes Legitimationsmedium) durch die Sitzungsleitung bestehen. Es muss dabei ausgeschlossen werden können, dass eine Zuschalte ausschließlich per Telefon bzw. Ton durch unbekannte Personen erfolgt.

Der Sitzungsleitung muss die Möglichkeit der An- und Abschaltung der Kameras eingeräumt werden.

Das Videokonferenzsystem sollte die Möglichkeit vorsehen, während der laufenden Videoverhandlung auch weitere Personen zur Gerichtsverhandlung hinzuzuziehen. So kann garantiert werden, dass etwa zusätzliche Zeugen bzw. Sachverständige kurzfristig gehört werden können. Damit eine solche Umsetzung für die betroffene Person auch reibungslos möglich ist, sollte die Einwahl über sämtliche Endgeräte per entsprechendem dann zu generierenden Einwahllink erfolgen können.

Die Nutzerfreundlichkeit und Praktikabilität müssen gewährleistet sein. Der Nutzer muss unproblematisch Zugang zu der angebotenen Lösung erhalten, sich schnell in der angebotenen

Lösung zurechtfinden und diese stabil und unterbrechungsfrei nutzen können. Ebenso sollte keine zusätzliche Software installiert werden müssen, die Lösung sollte daher aus dem Browser heraus ausgeführt werden können. Eine Nutzung ist zudem über mobile Geräte, wie Smartphones bzw. Tablets sicherzustellen.

Neben dem Komfort der Nutzung der eigentlichen Lösung ist aufgrund der Vielzahl von Anwendungen von Bedeutung, dass die verwendete Lösung interoperabel ist. Dies bedeutet, dass eine Verknüpfung mit anderem 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 hat bei der Schaffung eines bundeseinheitlichen Standards ein Datenschutzniveau zu gewährleisten, das höchsten Anforderungen genügt. Das setzt voraus, dass sowohl die Justiz als auch der jeweilige Betreiber der Videokonferenzsoftware 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 DS-GVO) 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 (vgl. die von der Kommission bereitgestellten Dokumente unter https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32010D0087).

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 DS-GVO) muss die Übermittlung durch geeignete Garantien gesichert sein.

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 darüber hinaus unbedingt sicherzustellen, dass bei den eingesetzten Videokonferenzsystemen das Risiko eines unbefugten Mithörens oder Mitschneidens durch Dritte oder Konferenzteilnehmer selbst ausgeschlossen ist. Dies gebietet z. B. etwa § 128a Abs. 3 Satz 1 ZPO. 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 Rechte 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.

Mit freundlichen Grüßen

Claudia Kalina-Kerschbaum
Geschäftsführerin

i. A. Pascal Heinzelmann
Referent