**Schrems II: Update zum Datenschutz bei Videokonferenzdiensten**

**Die Nutzung von Videokonferenzdiensten wirft auch Monate nach dem Beginn der Corona-Pandemie unbeantwortete datenschutzrechtliche Fragen auf. Die bereits im juris Magazin festgestellte Dynamik der Beurteilung besteht dabei weiterhin fort. So haben sich zwischenzeitlich zwar verschiedene Aufsichtsbehörden intensiver mit den Anforderungen an eine DSGVO-konforme Nutzung von Videodiensten beschäftigt, von einer abschließenden Klärung oder gesicherten Rechtslage kann jedoch keine Rede sein. Das „Schrems II“-Urteil des EuGH stellt die Nutzer von US-Diensten nun vor neue Herausforderungen.**

*Der Artikel behandelt ein wegen der sich stets verändernden Krisenlage hochaktuelles Thema. Nach Erscheinen können sich sehr schnell Änderungen der Sach- und Rechtslage ergeben. Unser Autor gibt die ihm bekannte Sach- und Rechtslage mit Stand vom 20.08.2020 wieder.*

**Die Rechtslage bleibt dynamisch**

Zumindest teilweise werden Videokonferenzdienste bzw. ihre Anbieter durch die Aufsichtsbehörden unterschiedlich bewertet. Die Berliner Datenschutzaufsicht geht beispielsweise in ihren neuen, überaus umfangreichen, [Hinweisen zu Videokonferenzdiensten für Berliner Verantwortliche](https://www.datenschutz-berlin.de/infothek-und-service/pressemitteilungen/#c98) davon aus, dass beim Anbieter Zoom „Zweifel an der Zulässigkeit“ bestehen. Währenddessen sieht der Landesdatenschutzbeauftragte von Baden-Württemberg das Unternehmen auf einem guten Weg und daher keinen „[Anlass mehr, seine an alle Schulen in Baden-Württemberg ausgesprochene Warnung länger aufrechtzuerhalten](https://www.baden-wuerttemberg.datenschutz.de/warnung-des-lfdi-wurde-gehoert-zoom-bessert-nach/)“. Diese beiden Ansichten sind nicht in Einklang zu bringen. Zur Klärung der Frage, welche Behörde richtig liegt, ist jedoch eine gerichtliche Entscheidung notwendig. Da bisher jedoch keine aufsichtsbehördlichen Maßnahmen gegen Verantwortliche, die Zoom einsetzen, bekannt geworden sind, erscheint eine zeitnahe Streitentscheidung unwahrscheinlich. Mit Rechtssicherheit ist also weiterhin nicht zu rechnen. Etwas mehr Licht ins Dunkel könnte jedoch eine Stellungnahme der Datenschutzkonferenz (DSK) bringen.

**Vorweg: Anforderungen an eine Auftragsverarbeitung**

Soweit Videokonferenzdienste nicht vom Verantwortlichen in Eigenregie betrieben werden, liegt meist eine Auftragsverarbeitung vor. Diese erfordert gemäß Art. 28 Abs. 9 DSGVO einen schriftlichen bzw. elektronischen Vertrag mit dem in Art. 28 Abs. 3 und Abs. 4 DSGVO näher bestimmten Inhalt. Aus Sicht der Berliner Datenschutzaufsicht erfüllten die Standardverträge vieler Anbieter diese gesetzlichen Anforderungen in der Vergangenheit jedoch nicht. Deswegen verwundert es wenig, dass die Behörde in ihren oben bereits erwähnten Hinweisen zum Ergebnis kommt, dass nur fünf von 17 geprüften Anbietern die Anforderungen der DSGVO erfüllen.

Zwingend erforderlich soll nach der Ansicht der Behörde unter anderem sein, dass der Anbieter vollständig weisungsgebunden handelt und personenbezogene Daten nicht zu eigenen Zwecken oder zu Zwecken Dritter verarbeitet. Außerdem wurde bemängelt, dass die Verträge oftmals nicht vorsähen, dass personenbezogene Daten sofort nach Abschluss der Leistungserbringung herausgegeben oder gelöscht wurden und, dass in diesem Kontext das Wahlrecht des Verantwortlichen nicht hinreichend berücksichtigt würde. Auch Vor-Ort-Prüfungen durch den Verantwortlichen und die Verpflichtung zur Bereitstellung erforderlicher Unterlagen würden oftmals unzulässig, beispielsweise durch Kostentragungspflichten zu Ungunsten des Verantwortlichen, eingeschränkt. Vor dem Hintergrund dieser umfassenden Kritik sollten Verantwortliche – insbesondere wenn sie unter der Aufsicht der Berliner Behörde stehen – prüfen, ob sie einen der geprüften Dienst nutzen und ggfs. notwendige Änderungen am bestehenden Vertrag veranlassen.

**juris PartnerModul IT-Recht** jetzt 4 Wochen gratis testen [Gratis testen](https://www.juris.de/jportal/allianz/nav/produktdetailsseiten/it-recht?id=produktdetails_52451.jsp)

**Neue Herausforderungen bei der Nutzung von US-Diensten**

Für Verantwortliche, die Anbieter aus den USA oder anderen Drittstaaten nutzen, hat das [Urteil des EuGH in der Rechtssache C-311/18](https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:62018CJ0311), auch bekannt als „Schrems II“-Urteil, eine weitere Baustelle geschaffen. In dieser Entscheidung, die [im juris Magazin bereits ausführlich kommentiert](https://www.juris.de/jportal/nav/juris_2015/aktuelles/magazin/facebook-privacy-shield-eugh-c-311-18.jsp) wurde, hat der EuGH den Angemessenheitsbeschluss für Datenübermittlungen in die USA, das sog. EU-US Privacy Shield, für ungültig erklärt. Zugleich hat das Gericht höhere Anforderungen an Datentransfers in Drittländer gestellt, wenn diese auf Basis von Standardvertragsklauseln stattfinden. Verantwortliche müssen demnach bei der Verwendung von Standardvertragsklauseln zunächst prüfen, ob die Vereinbarung der Klauseln ein hinreichendes Datenschutzniveau gewährleisten. Maßstab hierfür ist das europäischen Recht, insbesondere die EU-Grundrechtecharta.

In der Praxis dürfte es empfehlenswert sein, dem jeweiligen Empfänger zur Rechtslage im Zielland Fragen zu stellen und sich die Einhaltung der Standardvertragsklauseln zusichern zulassen. Ist dies zur Wahrung eines angemessenen Datenschutzniveaus nicht ausreichend, müssen zusätzliche Garantien geschaffen werden. In Bezug auf die USA ist davon auszugehen, dass insbesondere bei Unternehmen, die dem Foreign Intelligence Surveillance Act (FISA), der Executive Order (EO) 12.333 oder dem CLOUD Act unterliegen, ein angemessenes Datenschutzniveau durch die Vereinbarung von Standardvertragsklauseln allein nicht gewährleistet werden kann. Folglich sind zusätzliche Garantien erforderlich. Dies wirft die Frage auf, worin solche allgemein und bei Videodiensten im Speziellen bestehen könnten.

**Zusätzliche Garantien bei Videodiensten**

Eine einfache Lösung für diese Problematik könnte bei Videodiensten in einer Ende-zu-Ende-Verschlüsselung sämtlicher Kommunikationsinhalte bestehen. Die Inhalte einer Videokonferenz wären dann nur von den jeweiligen Teilnehmern einsehbar. Eine unzulässige Datenverarbeitung durch den Diensteanbieter wäre technisch ausgeschlossen. Allerdings ist eine Ende-zu-Ende-Verschlüsselung bei Videokonferenzdiensten nicht Stand der Technik und darüber hinaus technisch limitiert. Gleichwohl gibt es jedoch Anbieter, die bereits eine Ende-zu-Ende-Verschlüsselung ermöglichen beziehungsweise, wie z.B. Zoom, an einer solchen arbeiten.

Doch selbst soweit eine Ende-zu-Ende-Verschlüsselung vorliegt, dürften die im Kontext einer Videokonferenz anfallenden Verbindungsdaten (sog. Metadaten), einen Personenbezug aufweisen und es läge dennoch ein Datentransfer in ein Drittland vor. Schließlich erlauben insbesondere Metadaten über Kommunikationsvorgänge sehr viele Rückschlüsse. Der Bundesbeauftragte für den Datenschutz (BfDI) hat dies zuletzt im Zusammenhang mit WhatsApp in einem [Schreiben an alle Bundesministerien und obersten Bundesbehörden](https://www.bfdi.bund.de/DE/Infothek/Transparenz/Stellungnahmen/2020/Rundschreiben-Nutzung-WhatsApp.html) betont und eine dienstliche Nutzung in seinem Zuständigkeitsbereich für unzulässig erklärt. Eine Ende-zu-Ende-Verschlüsselung ohne weitere Garantien dürfte daher zumindest im Kontext von Videokonferenzen unzureichend sein. Neben weiteren technischen Maßnahmen sollten Verantwortliche deswegen erwägen mit den Anbietern von Videokonferenzdiensten zusätzliche vertragliche Garantien zu vereinbaren. Diese können beispielsweise in einer Verpflichtung des Anbieters bestehen keine Hintertüren in die eingesetzte Software einzubauen oder staatliche Auskunftsanfragen in einem vertraglich vereinbarten Prozess zu bearbeiten. Auch Gerichtsstandsvereinbarungen und Vertragsstrafen können zusätzliche Garantien darstellen. Darüber hinaus sollten Verantwortliche klären, inwieweit der jeweilige Anbieter Überwachungsgesetzen unterworfen ist und, ob die Gesetze mit europäischen Maßstäben vereinbar sind. Inwieweit US-Anbieter sich auf derartige Maßnahmen einlassen und ob diese wirklich ausreichend sind, bleibt allerdings abzuwarten. Dies darf Verantwortliche jedoch nicht dazu verleiten untätig zu bleiben, da von Betroffenen-Initiativen bereits [erste Beschwerden zu US-Transfers bei den Aufsichtsbehörden eingelegt](https://noyb.eu/de/101-beschwerden-zu-eu-us-transfers-eingereicht) wurden.

**Nicht in Aussicht: EU-US Privacy Shield 2.0**

Eine Lösung, welche die praktischen Schwierigkeiten von zusätzlichen Garantien bei Standardvertragsklauseln umgeht, könnte die Vereinbarung eines neuen Datenschutzabkommens mit den USA bzw. eine Überarbeitung des EU-US Privacy Shield nach den Vorgaben des EuGH sein. Doch obwohl diesbezüglich [erste Verhandlungen aufgenommen](https://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=684836) wurden, ist eine zeitnahe Lösung aus mehreren Gründen unwahrscheinlich. Als ausgeschlossen erscheint insoweit zunächst eine Vereinbarung vor den US-Präsidentschaftswahlen im November. Selbst wenn sich Joe Biden dann gegenüber Donald Trump durchsetzen sollte, ist jedoch eher mit langwierigen Verhandlungen, als mit einer schnellen Lösung zu rechnen. Ein neues Abkommen, das den Anforderungen des EuGH genügt, würde nämlich ein Einschränkung der US-Überwachungsgesetze gegenüber EU-Bürgern erfordern. Hierzu dürfte selbst ein Präsident Biden jedoch nicht ohne weiteres bereit sein. Nachdem der EuGH mit dem EU-US Privacy Shield zuletzt und mit dem Safe Harbour Abkommen bereits im Jahr 2015 bereits zwei Angemessenheitsbeschlüsse der EU-Kommission gekippt hat, dürfte von EU-Seite gleichzeitig wenig Verhandlungsspielraum bestehen.

**Fazit**

**Um der aktuellen Entwicklung Rechnung zu tragen, müssen Verantwortliche zunächst die Verträge zur Auftragsverarbeitung mit dem Anbieter auf Übereinstimmung mit den Anforderungen der DSGVO prüfen. Dies mag zunächst trivial klingen, verlangt dem Verantwortlichen jedoch einiges ab. Darüber hinaus müssen Verantwortliche prüfen, ob bei der Nutzung des Videokonferenzdiensts Daten auf Basis von Standardvertragsklauseln in Drittländer, insbesondere die USA, übermittelt werden. Ist dies der Fall müssen – wie bei anderen US-Transfers – zusätzliche Garantien für eine Einhaltung der Klauseln geschaffen werden. Insbesondere im US-Kontext kann dies schwierig bis unmöglich sein. Darauf, dass es zeitnah einen Nachfolger für das EU-US Privacy Shield gibt, sollten sich Unternehmen indes aufgrund der politischen Lage in den USA nicht verlassen.**