

Videokonferenz-Tools und Datenschutzrecht: Prozesse prüfen und Maßnahmen ergreifen

Categories : [Datenschutzrecht](#)

Tagged as : [C-311/18](#), [C-362/14](#), [Datenschutzkonzept](#), [Ende-zu-Ende Verschlüsselung](#), [EU-US Privacy Shield](#), [internationaler Datentransfer](#), [MS Teams](#), [personenbezogene Daten](#), [SaaS](#), [Safe-Harbor-Abkommen](#), [Skype](#), [Software as a Service](#), [Transportverschlüsselung](#), [Videokonferenz](#), [Zoom](#)

Date : 9. September 2020

Befördert durch die Corona-Pandemie greifen Unternehmen verstärkt auf Videokonferenz-Tools wie Zoom, Microsoft Teams oder Skype zurück. Auch Videokonferenzen sind im Datenschutzkonzept eines Unternehmens zu berücksichtigen – und ein Urteil ([Schrems-II-Urteil](#) - Rs. C-311/18) des [Europäischen Gerichtshofs](#) (EuGH) vom 16.7.2020 ([wir berichteten](#)) macht in vielen Unternehmen Anpassungen notwendig.

Datenübertragung zwischen der EU und den USA

Viele der Unternehmen, die Videokonferenz-Tools anbieten, sind in „Drittländern“ – also Staaten außerhalb der EU – ansässig. Bei der Nutzung ihrer Dienste werden personenbezogene Daten verarbeitet, etwa Namen und E-Mailadressen von Teilnehmern oder deren Stimme und Videobild. Um bei der Datenübermittlung die Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf Schutz personenbezogener Daten gem. [Art. 8 Europäischen Grundrechtecharta](#) zu wahren, verlangt die [Datenschutz-Grundverordnung](#) (DS-GVO), dass ein angemessenes Schutzniveau gewährleistet wird ([Art. 44 DS-GVO](#)).

Die Übermittlung personenbezogener Daten in ein Drittland kann zum Beispiel auf der Grundlage eines sog. Angemessenheitsbeschlusses der EU-Kommission stattfinden ([Art. 45 DS-GVO](#)). Zwischen 2000 und 2015 galt ein solcher Beschluss zwischen den USA und der EU für Unternehmen, die sich dem [Safe-Harbor-Abkommen](#) unterworfen haben. Der EuGH erklärte dieses Abkommen im Oktober 2015 für [ungültig](#) (Rs. C-362/14), da es Probleme bei den Zugriffsrechten von US-Behörden, der Selbstzertifizierung und der Überprüfung der Einhaltung von Datenschutzstandards gab ([wir berichteten](#)).

2016 trat das [EU-US-Privacy Shield](#) in Kraft, das diese Probleme beheben sollte. Am 16.7.2020 erklärte der EuGH jedoch auch dieses Abkommen für ungültig (Az. C-311/18). Hauptgrund für die Entscheidung war, ähnlich wie schon beim Safe-Harbor-Abkommen, Überwachungsprogramme und Zugriffsrechte US-amerikanischer Behörden. Das bedeutet, dass eine Datenübermittlung in die USA nicht mehr auf einen Angemessenheitsbeschluss der EU-Kommission gestützt werden kann. Es braucht daher eine andere Grundlage für den internationalen Datentransfer.

In Frage kommen „geeignete Garantien“ im Sinne des [Art. 46 DS-GVO](#), von denen insbesondere die Standardvertragsklauseln verbreitet Anwendung finden. Deren schlichte Übernahme genügt jedoch spätestens seit der jüngsten EuGH-Entscheidung ebenfalls nicht mehr. Der EuGH hat klargestellt, dass jeder Verantwortliche im Einzelfall prüfen muss, ob die Vereinbarung der Standardvertragsklauseln mit dem Empfänger im Drittland ausreicht oder weitere Vorkehrungen getroffen werden müssen. Das können z.B. zusätzliche Vereinbarungen oder auch technische und organisatorische Schutzmaßnahmen sein ([wir berichteten](#)).

Das heißt: Alle Verträge, die auf die Standardvertragsklauseln setzen, müssen auf den Prüfstand und Unternehmen, die für den Transfer bisher auf das Privacy Shield verwiesen haben, müssen ihre Datenschutzerklärungen überarbeiten.

Video-Konferenzen und Datenschutz

In der Regel werden Videokonferenz-Tools als Software as a Service (SaaS) angeboten; das heißt, der Dienstleister stellt die Plattform/Infrastruktur selbst bereit. Dabei fungieren die Anbieter gem. [Art. 4 Nr. 8 DS-GVO](#) als Auftragsverarbeiter und es wird nach [Art. 28 Abs. 3 DS-GVO](#) ein Vertrag über die Auftragsverarbeitung zwischen Dienstleister und Nutzer abgeschlossen. Verantwortlich im Sinne der DS-GVO und rechenschaftspflichtig bleibt aber der Nutzer.

Doch die Datenübermittlung bei Videokonferenz-Tools birgt Risiken: Im April 2020 wurde etwa bekannt, dass aufgrund einer [Sicherheitslücke](#) bei dem Unternehmen Zoom sensible Daten an Facebook weitergegeben wurden. Ein weiterer problematischer Punkt besteht darin, dass die meisten Anbieter nur eine Transportverschlüsselung, jedoch keine Ende-zu-Ende Verschlüsselung benutzen. Unternehmen sollten daher, nicht zuletzt im Lichte der Entscheidung des EuGH, Maßnahmen ergreifen, um den Umfang der Verarbeitung personenbezogener Daten zu minimieren ([Art. 5 Abs. 1 lit. c DS-GVO](#)) und die eingesetzten Mittel möglichst datenschutzfreundlich und vor allem sicher zu gestalten ([Art. 25 , 32 DS-GVO](#)).

Maßnahmen ergreifen

Der Umgang mit übermittelten, personenbezogenen Daten im Hinblick auf Drittländer gestaltet sich komplex. Umso wichtiger ist es, dass Unternehmen Maßnahmen ergreifen, um die Daten bestmöglich zu schützen.

Zusätzlich zu dem AV-Vertrag sollte daher der Verarbeitungsprozess für die Nutzung der Konferenzdienste im Verzeichnis von Verarbeitungstätigkeiten ([Art. 30 DS-GVO](#)) festgehalten werden. Schon bei der Auswahl des Anbieters sollten Datenschutzaspekte miteinbezogen werden. Die Organisatoren/Verantwortlichen im Unternehmen sollten nach Auswahl des Anbieters die Einstellungen im Vorfeld der Konferenzen datenschutzfreundlich gestalten. Das umfasst Einstellungen zu Verschlüsselungs-, Protokollierungs-, Tracking- und Aufzeichnungsfunktionen.

Der Arbeitgeber sollte außerdem seiner Informationspflicht nach [Art. 13 DS-GVO](#) nachkommen, indem er Mitarbeiter schult und Informationen über Art und Umfang der Datenverarbeitung bereitstellt. Bei dieser Gelegenheit werden die betroffenen Mitarbeiter über den Umgang mit ihren personenbezogenen Daten im Zusammenhang mit Videokonferenzen sensibilisiert. Hierbei kann die umfangreiche Praxishilfe der Gesellschaft für Datenschutz und Datensicherheit e.V. vom April 2020 mit dem Titel [Videokonferenzen und Datenschutz](#) eine Hilfestellung sein.

Ansprechpartner: [Tobias Sengenberger](#)/[Alexander Bartsch](#)/[Thomas Schmeding](#)/[Dr. Maximilian Festl-Wietek](#)