ORIENTIERUNGSHILFE
ZUM EINSATZ WEBBASIERTER VIDEOKONFERENZSYSTEME

Stand: September 2020

Die Corona-bedingten Maßnahmen haben dazu geführt, dass ein erheblicher Anteil der Beschäftigten berufliche Aufgaben von zuhause aus erledigen muss. Mit einer vollständigen Rückkehr zum status quo ante ist in absehbarer Zeit nicht zu rechnen. Unabhängig davon hat sich in den vergangenen Monaten gezeigt, dass in vielen Bereichen bzw. für viele Tätigkeiten eine solche Verlagerung der Arbeit an einen privaten Arbeitsplatz technisch zu bewältigen und arbeitsorganisatorisch ohne durchgreifende Nachteile umzusetzen ist und überdies den Beschäftigten durchaus entgegenkommen kann. Deshalb wird voraussichtlich dauerhaft mit einem deutlich größeren Anteil von Heimarbeit auch in den Rundfunkanstalten und ihren Beteiligungsunternehmen zu rechnen sein.

Diese Entwicklung führt unter anderem dazu, dass es erforderlich – aber auch möglich – ist, Arbeitsbesprechungen, Sitzungen und Konferenzen häufiger als in der Vergangenheit auf elektronischem Weg durchzuführen. Dafür stehen unterschiedliche Videokonferenzsysteme zur Verfügung, die den Teilnehmern eine virtuelle Sitzungspräsenz ermöglichen. Dabei muss der jeweilige Verantwortliche allerdings nicht zuletzt für einen datenschutzkonformen Einsatz solcher Anwendungen sorgen. Die folgende Orientierungshilfe enthält Hinweise auf die Gesichtspunkte, die er dabei besonders zu berücksichtigen hat.

I. Ausgangslage

Neben dem ARD-eigenen, vom Sternpunkt administrierten Konferenzsystem, das das rundfunkinterne Leitungsnetz nutzt, setzen die Rundfunkanstalten bislang unterschiedliche Videokonferenzsysteme ein, insbesondere

- Skype Broadcast / Skype for Business
- Microsoft Teams
- Rocketchat
- Jitsi
- Webex
- Fast Viewer

Daneben gestatten einige Rundfunkanstalten im Einzelfall die Nutzung sonstiger Systeme wie etwa Zoom, sofern es um die Teilnahme an einer von einem Dritten organisierten Konferenz geht.

Im Rahmen des Einsatzes von Videokonferenzsystemen werden insbesondere folgende personenbezogene Daten verarbeitet:

- Namen und Kontaktdaten der Videokonferenz-Teilnehmer
- Inhalte der Videokonferenz (Ton-, Bild- und Videoübertragung/-aufzeichnung); dazu können auch besonders sensible Daten im Sinne von Art. 9 DSGVO gehören (z.B. körperliche Eigenschaften, Hautfarbe, politische Einstellung etc.)
- Metadaten (z.B. Verbindungsdaten)
- ggf. Chatverläufe.

Je nachdem, um welches System bzw. um welchen Anbieter es sich handelt, werden diese Daten ganz oder teilweise auf Server in Nicht-EU-Staaten, insbesondere in den USA übermittelt.

II. Anforderungen in datenschutzrechtlicher Hinsicht

1. Vorprüfung

Vor einer Auswahlentscheidung sollte der Verantwortliche im Sinne der allgemeinen datenschutzrechtlichen Gebote zum Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen (Art. 25 DSGVO) zunächst die Anforderungen definieren, die das gewünschte Videokonferenzsystem in jedem Falle erfüllen soll. Daran ist der Leistungsumfang der unterschiedlichen (kostenlosen und kostenpflichtigen) Videokonferenzsysteme zu messen.

2. Datenschutzrechtliche Beurteilung

Das gewünschte Videokonferenzsystem muss der Verantwortliche daraufhin überprüfen, ob es alle zwingenden datenschutzrechtlichen Anforderungen wie insbesondere die Grundsätze für die Verarbeitung personenbezogener Daten (Art. 5 DSGVO) sowie für die Rechtmäßigkeit der Verarbeitung (Art. 6 DSGVO) erfüllt. Unter den in Art. 35 DSGVO genannten Voraussetzungen muss er dazu gegebenenfalls eine Datenschutzfolgenabschätzung durchführen. Eine solche ist jedenfalls dann erforderlich, wenn das betreffende System den Einsatz neuer Technologien wie Sprach-, Gesichts- oder Stimmenerkennung oder die Transkription ermöglicht bzw. vorsieht.

3. Auftragsverarbeitungsvertrag und technisch-organisatorische Maßnahmen

Die Rundfunkanstalten setzen den Anbieter des gewünschten Videokonferenzsystems in datenschutzrechtlicher Hinsicht als Auftragsverarbeiter ein. Grundlage dafür ist ein Auftragsverarbeitungsvertrag, der die Anforderungen des Art. 28 DSGVO, insb. des Absatzes 3 lit. a) – g) DSGVO erfüllen muss. Dementsprechend muss der Vertrag technische und organisatorische Maßnahmen vorsehen oder ermöglichen, die die in Art. 28 Abs. 3 DSGVO genannten Vorgaben zur Datensicherheit gewährleisten. Dazu gehören namentlich folgende Anforderungen:

- Ausschalten des Aktivitätstrackings von Teilnehmern,
- Manuelle Datenschutzeinstellungen entsprechend der internen Vorgaben der Rundfunkanstalt,
- Nutzung nur für einen konkreten Teilnehmerkreis ermöglichen,
- Ende-zu-Ende-verschlüsselte Datenübertragung ermöglichen,
- Deaktivierung von Mitschnitten einer Videokonferenz oder Informationen an die Teilnehmer vorab über die Aufzeichnung,
- Automatische bzw. entsprechend den Aufbewahrungsbestimmungen festgelegte Löschung eventueller Aufzeichnungen bzw. Mitschnitte nach einer Videokonferenz,
- Deaktivierung von Datensammlungen der einzelnen Nutzer (Nutzungsprofile),
- Ggfs. Aktivierung einer automatischen Hintergrund-Weichzeichnung oder eines virtuellen Hintergrunds,
- Möglichkeit zum Unkenntlichmachen von Informationen, die nicht jedem Teilnehmer zur Verfügung stehen sollten,
- Nutzung von Zugangsdaten nur für einen bzw. bestimmte Teilnehmer.

Sofern der Anbieter seinen Sitz in einem Nicht-EU-Staat hat bzw. die Daten in einem Nicht-EU-Staat verarbeitet, muss der Verantwortliche überdies prüfen, ob die Datenübermittlung in das Drittland im Einklang mit den Artt. 44 ff. DSGVO steht. Da der EuGH mit Urteil vom 16. Juli 2020 - C-311/18 - das EU-US-Abkommen Privacy Shield für rechtswidrig erklärt hat, stellt sich diese Frage vor allem mit Blick auf US-amerikanische Anbieter.

4. Dokumentation und Information
Der Verantwortliche muss die Datenverarbeitung im Rahmen des Einsatzes von Videokonferenzsystemen gemäß Art. 30 DSGVO in seinem Verarbeitungsverzeichnis dokumentieren und außerdem seine Beschäftigten gem. Artt. 12 ff. DSGVO über die mit dem Einsatz eines solchen Systems verbundenen datenschutzrelevanten Aspekte umfassend und verständlich informieren.

III. Interne Regularien

Um die Einhaltung der datenschutzrechtlichen Anforderungen zu gewährleisten, empfiehlt sich ein Regelwerk (Dienstanweisung, Betriebs- oder Dienstvereinbarung etc.), das die wesentlichen Vorgaben zum Einsatz eines Videokonferenzsystems zusammenfasst. Dabei muss der Verantwortliche in geeigneter Weise gewährleisten, dass das Regelwerk nicht nur (etwa über eine Dienstanweisung oder Dienstvereinbarung) seine Arbeitnehmer, sondern auch die in freier Mitarbeit beschäftigten Personen verpflichtet. Dies bietet sich insbesondere an, soweit das vom jeweiligen Anbieter zur Verfügung gestellte Videokonferenzsystem datenschutzrechtlich sinnvolle oder erforderliche technische Vorkehrungen nur fakultativ vorsieht.

Zu den dort zu regelnden Punkten können insbesondere die folgenden gehören:

- Überblick über die datenschutzrechtlichen Risiken bei der Nutzung webbasierter Videokonferenzsysteme (Information und Sensibilisierung).
- Freigabeverfahren, das festlegt,
  - welche Videokonferenzsysteme in welchem Umfang freigegeben sind,
  - welche Voraussetzungen an die Freigabe gestellt sind und
  - wie technisch gewährleistet wird, dass die Beschäftigten andere als die freigegebenen Videokonferenzsysteme für dienstliche Zwecke nicht einsetzen können.
- Datenschutzfreundlichste Voreinstellung (bspw. Kamera und Mikrofon deaktiviert) als vorgegebener Standard.
- Vorgaben zum Funktionsumfang und zu Zugriffsberechtigungen, darunter etwa die Verpflichtung zur Prüfung, ob anstatt einer Video- eine Telefonkonferenz ausreicht, etwaiges Verbot der Aufzeichnungsfunktion (Mitschnitt, Screenshot, Fotografie) ohne ausdrückliche Einwilligung.
- Kontrollierter und individueller Zugang zur jeweiligen Konferenz (bspw. Registrierung, Passwort).
- Geeignete und verlässliche Information aller Konferenzteilnehmer.
- Gewährleistung, dass alle personenbezogenen Daten nach der Konferenz effektiv gelöscht werden.
- Ausschluss einer Auswertung der Daten zur Verhaltens- oder Leistungskontrolle.

Gez. Dr. Reinhart Binder