Videokonferenz

Eine **Videokonferenz** ist eine audiovisuelle Fernkommunikation mehrerer Personen. Bei nur zwei beteiligten Personen wird auch von einem **Bildtelefonat** (bzw. **Bildtelefonie**) gesprochen. Bei einer rein auditiven Kommunikation handelt es sich um eine **Telefonkonferenz**

Aus Datenschutzsicht sind die beteiligten Personen in aller Regel betroffene Personen deren Personenbezogene Daten, dazu zählen auch Bild- und Sprachaufnahmen, verarbeitet werden.

Als Rechtfertigungstatbestand für die Rechtmäßigkeit der Verarbeitung wird in aller Regel die Einwilligung in Betracht kommen. Denkbar sind aber auch andere Tatbestände. Soweit es sich bei den betroffenen Personen um Beschäftigte handelt, sind die Besonderheiten des Beschäftigtendatenschutzes zu beachten. Das gilt in verstärktem Maße für Bewerbungsgespräche.[1)]

Komplex wird eine Videokonferenz, weil es häufig mehrere Verantwortliche (zum Beispiel die Arbeitgeber der konferierenden Personen) gibt und zusätzlich Dienstanbieter, die die Infrastruktur zur Verfügung stellen. Das erfordert entsprechende vertragliche Regelungen und meist auch eine Dokumentation im VVT.

Eine maßgebliche Rolle bei der Sicherstellung des Datenschutzes bei Videokonferenzen hat das Videokonferenzsystem.

Gefahren von Videokonferenzen

Die Vertraulichkeit von Videokonferenzen ist in mehrfacher Hinsicht problematisch:

- Teilnehmer der Konferenz können die Konferenz mitschneiden. Jedes brauchbare Videokonferenzsystem gibt zwar allen Teilnehmer ein Signal, wenn aufgezeichnet wird. Allerdings gilt das jeweils nur für die in das jeweilige System integrierte Aufzeichnungsfunktion. Es ist aber mit fast allen Endgeräten möglich, die Bildschirmanzeige als Video aufzuzeichnen, wobei kaum Qualitätsverluste entstehen. Selbst wenn das unterbunden werden könnte, wäre es mit etwas größeren Qualitätsverlusten klassisch analog möglich, eine Kamera vor einen Bildschirm zu stellen und dann mit der Kamera den Bildschirm aufzuzeichnen.
- Anbieter des Videokonferenzsystems haben technisch Zugriff auf die Videokonferenz, wenn sie einen Teil der Infrastruktur stellen(SaaS). Ausnahme wäre eine Ende-zu-Ende-Verschlüsselung durch die „lediglich“ die Metadaten dem Anbieter zur Kenntnis gelangen. Ein gewisser Schutz lässt sich hier durch geeignete Regelungen im Auftragsverarbeitungsvertrag leisten allerdings technisch sind keine Vorkehrungen möglich. Bei komplett selbstgehosteten Systemen sollte der Anbieter dagegen keinen Zugriff auf die Daten haben; jedenfalls gibt es dafür in der Regel keine technische Notwendigkeit.
- Die Organisation (also das Unternehmen oder die öffentliche Einrichtung), die das Videokonferenzsystem nutzt beziehungsweise zur Verfügung stellt hat in der Regel zumindest Zugriff auf die Metadaten; möglicherweise auch auf die Inhalte der Videokonferenzen. Da beim professionellen Einsatz von Videokonferenzen vorrangig Beschäftigte dieser Organisation Teilnehmer der Videokonferenzen sein werden, ist diese Zugriffsmöglichkeit im Rahmen des Beschäftigtendatenschutzes von großer Bedeutung.
- Dritte (Hacker, Geheimdienste, Trolle-Zoombombing)

Generelle Hinweise

Bei Videokonferenzen sollte grundsätzlich beachtet werden:

- Gute Audioqualität ist für eine erfolgreiche Kommunikation essentiell:
  - Optimal ist ein Einsatz von Headsets mit Mikrofon. Das Mikrophon am Kopf statt deutlich weiter entfernt am Laptop verbessert die Tonqualität deutlich.
  - Mindestens sollten aber Kopfhörer verwendet werden-nicht für einen selber, sondern für die anderen Teilnehmer, die ansonsten von Rückkopplungen massiv gestört werden. Die Kopfhörer müssen keine High-End-Geräte sein. Die meisten Laptops haben noch Ausgänge für Klinkenstecker, so dass nahezu alle Kopfhörer der letzten Jahrzehnte verwendet werden können; zB auch von alten Handys.
  - Wer nichts sagen will - Mikrofon ausschalten, um Nebengeräusche zu verhindern.
- Die Bildqualität hat häufig eine untergeordnete Bedeutung:
  - Übertrieben hohe Auflösungen sollten vermieden werden - im Interesse von Datenschutz und IT-Systemen (Bandbreite).
  - Die meisten Kameras zeigen bei einer guten Ausleuchtung deutlich bessere Ergebnisse, während bei schwacher Ausleuchtung nur sehr gute Kameras überzeugen. Die Lichtquelle sollte ausreichend stark sein und zur Vermeidung von Schattenwürfen möglichst von vorn und nicht von oben wirken.
  - Gegenlicht vermeiden, also lieber zum Fenster schauen als mit dem Rücken zum Fenster.
  - Bei sehr schlechter Bildqualität und wenn es auf das Bild nicht ankommt, kann die Kamera auch ausgeschaltet werden.
  - Die Kamera sollte einen festen Stand haben.
- Ein neutraler Hintergrund ist zweckmäßig - möglichst ohne elektronische Helfer[2)] aber die Entwicklung der virtuellen Hintergründe ist weit vorangekommen.
- Möglichst ungestörte Umgebung. Türen sollten geschlossen sein, evtl. auch von außen mit einem Hinweisschild versehen, dass gerade eine Videokonferenz läuft.
- Essen während einer Videokonferenz sollte tabu sein. Trinken nur bei ausgeschaltetem Mikrofon. Generell bedenken, dass die anderen teilnehmenden Personen einem direkt ins Gesicht sehen.
- Der eigene Status (online, offline, in Videokonferenz etc.) sollte nicht allgemein bekannt sein

Weblinks

- Das Lemma in der Wikipedia

Artikel

1)

Vgl. datenschutzbeauftragter-info.de:Das Videointerview im Bewerbungsverfahren.

2)

Zu den Gefahren, wenn Tools für optische Effekte vorhanden sind, siehe Ursula Scheer: Chefkartoffel bei faz.net, abgerufen am 1.4.2020.