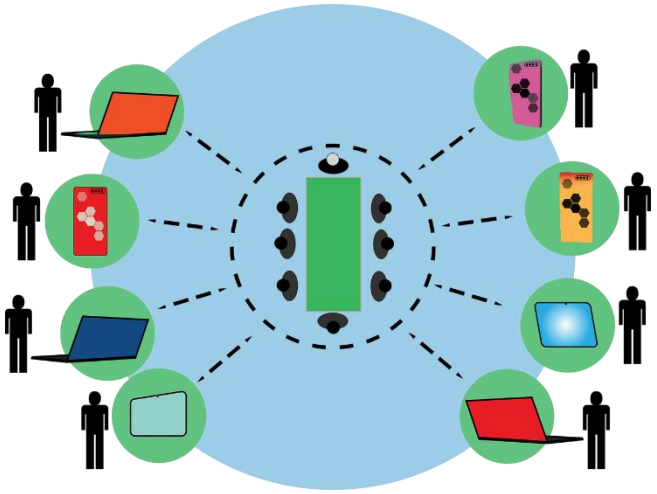

Zoom, GoTo-Meeting, MS Teams und andere technische Tools für Videokonferenzen

Videokonferenzen sind derzeit eine Möglichkeit, mit Kunden oder Lieferanten geschäftliche Kontakte abzuwickeln oder im Mitarbeiter*Innen-Team Besprechungen abzuhalten.

Grundsätzliche datenschutzrechtliche Implikationen

Bei **Videokonferenzen** werden regelmäßig vom Verantwortlichen (Veranstalter) **personenbezogene Daten der Teilnehmer verarbeitet**, insbes. Teilnehmerlisten, Passwörter etc...

Die **Rechtmäßigkeit** der Datenverarbeitung ergibt sich daraus, dass die Verarbeitung zur **Erfüllung eines Vertrages notwendig ist (Art 6 Abs 1 lit b DSGVO)**, dessen Vertragspartei der Betroffene bzw. der betroffene Mitarbeiter des Vertragspartners ist, wenn es zB ein Seminar über ein Videokonferenztool abgehalten wird, oder das **berechtigte Interesse** des Dienstgebers, mit seinem Mitarbeiter*Innen effizient zu kommunizieren (**Art 6 Abs 1 lit f DSGVO**), wenn Team-Meetings über Videokonferenzen abgehalten werden.

Auch die (freiwillige, informierte und jederzeit widerrufbare) **Einwilligung** (Art 6 Abs 1 lit a DSGVO) kommt als Rechtsgrundlage in betracht, wobei jedoch die Einwilligung in entsprechender Form nachweisbar sein muss und auch an die Formulierung derselben hohe Anforderungen gestellt werden.

Der **Videokonferenzanbieter** führte für den Verantworltichen eine Verarbeitungstätigkeit durch; er ist **Auftragsverarbeiter** für den Verantwortlichen iSd Art 28 DSGVO und daher ist eine entsprechende dokumentierte **Vereinbarung über Auftragsverarbeitungstätigkeiten** mit dem Anbieter zu schließen.

Beachten Sie auch, dass diese neue Art der Kommunikation als Verarbeitungstätigkeit in das **Verzeichnis der Verarbeitungstätigkeiten** aufgenommen werden muss.

Weiters ist zu bedenken, dass von den Teilnehmern an der Konferenz / dem Meeting personenbezogene Daten verarbeitet werden, und die Teilnehmer nicht in Kenntnis sind, wie die Verarbeitung der Daten erfolgt. Eine **Datenschutzinformation iSd Art 13 DSGVO für Videokonferenzen** ist daher notwendig, und sollte den Teilnehmern (und auch den Referenten) vorab zur Verfügung gestellt werden.

Rollenverteilung mehrere „Verantwortlicher“

Wenn mehrere Unternehmen bzw. Mitarbeiter*Innen aus unterschiedlichen Unternehmen teilnehmen, sollte vorab geklärt werden, welche **Rolle** welches Unternehmen hat. Wer ist der **Verantwortliche** in datenschutzrechtlicher Hinsicht? Sind alle teilnehmenden Unternehmen **gemeinsame Verantwortliche**?

Datenübermittlungen in Drittländer

Zu beachten ist auch, dass **personenbezogene Daten bei den meisten Anbietern in Länder außerhalb der EU** (oder gelichgestellter Staaten) **übertragen werden**; es ist durch **entsprechende Maßnahmen** sicherzustellen, dass dies zulässig ist, oder zB bei Anbietern aus den USA zu prüfen, ob diese dem EU-US-Privacy-Shield unterliegen, oder nicht.

Prinzip der Datenminimierung

Überlegen Sie, welche **Kommunkationsmittel** neben Videokonferenzen für die Handlungen, die notwendig sind, sonst noch in Frage kommen. Wenn zB nur zwei Personen teilnehmen, dann wird es nicht erforderlich sein, auch das Bild der Person zu sehen, und mit dieser über eine Videokonferenz „zu **telefonieren**“. Es gibt auch andere

Möglichkeiten, Dokumente oder Präsentationen zu teilen, ohne Videos (aus dem Home-Office oder dem Office) zu übertragen.

Wenn **Funktionen eines Tools**, die **nicht** für die Abwicklung **erforderlich** sind, genutzt werden (sollen), dann wird es mE nur möglich sein, dies mit einer informierten, freiwilligen und jederzeit widerrufbaren sowie nachweisbaren **Einwilligung** der betroffenen Personen abzuwickeln.

Es wird zB bei Seminaren, die abgehalten werden, nicht notwendig sein, dass die **Teilnehmerliste** offen im Display der Teilnehmer erscheint, oder der Veranstalter gibt die Möglichkeit, freiwillig den Namen (oder auch ein Pseudonym) anzugeben, und muss jedenfalls darüber informieren, welche Folgen die Angabe des Namens hat (zB ob dieser für alle anderen Teilnehmer sichtbar ist, oder nicht). Gleiches gilt für andere Identifkationselemente, wie zB die **E-Mail-Adresse** der teilnehmenden Personen.

Datenschutzfreundliche Grundeinstellungen

Der Veranstalter der Videokonferenz hat dafür Sorge zu tragen, dass die Voreinstellungen in einer Art erfolgen, die es ermöglicht, nur die erforderlichen Daten zu verarbeiten, die von den Teilnehmern zur Verfügung gestellt werden.

Verschiedene Anbieter bieten verschiedene Möglichkeiten, die von einem **Aufmerksamkeitstracking** von Teilnehmern (die Maus eines Teilnehmers wird nicht mehr bewegt und der Seminarleiter erkennt dies) bis zu **Berichten über Systemabstürze** bei Teilnehmer oder ähnlichen Features geht.

Der Veranwortliche mss sich im Detail überlegen, ob das **Sceensharing** für Teilnehmer zugelassen werden soll, oder nicht, und dies wird vom Format der Videokonferenz abhängig sein. Bei einerm Seminar wird dies mE nicht nötig sein, bei einem Teammeeting unter Kollegen oder einer Besprechung von Kunden und Lieferanten uU aber schon.

Die **Aufzeichnung der Videokonferenz** sollte mE unterbunden werden.

Wenn es **Aufzeichnungen von Chat-Verläufen**, **Beiträgen von Teilnehmern** oder **übermittelte Dateien** (zB Screenshots oder Dokumente) gibt, dann dürfen diese nur so lange aufbewahrt werden, wie dies zur **Erfüllung des konkreten Zweckes** erforderlich ist. Dies wird daher nicht über die Videokonfernz an sich definiert, sondern den Art des Inhaltes (Meeting unter Mitarbeiter*Innen, Teilnahme an einem Seminar ...)

Zu prüfen ist auch, ob eine **verschlüsselte Übertragung** möglich ist, und diese Möglichkeit sollte auch genutzt werden. Für Inhalte, die personenbezogene Daten iSd Art 9 DSGVO darstellen, ist dies mE eine unbedingte Notwendigkeit.

Die Teilnehmer der Videokonferenz sollten auch darauf achten, welche Dinge im **Hintergrund des übertragenen Videos** (für andere Teilnehmer) sichtbar sind, wobei es hier nicht nur um die Dekoration im Heim-Büro geht, sondern auch um etwaige Charts oder sonstige Dinge, die auch im Büro im Hintergrund sichtbar sein können, und deren Übertragung für die anderen Teilnehmer zwar interessant sein kann, aber einen unbefugten Zugriff auf Daten darstellen kann. Manche Videokonferenztools bieten die Möglichkeit, einen **neutralen Hintergrund** auszuwählen.

Datenschutzfolgen-Abschätzung

Beim Einsatz von Videokonferenztools ist auch zu prüfen, ob eine DSFA durchzuführen ist, da „neue Technologien" zum Einsatz kommen, und das Risiko des Einsatzes jedenfalls zu bewerten ist. Gegebenenfalls ist eine **DSFA** durchzuführen.

Auch die unterschiedliche technischen Möglichkeiten (Aufmerksamkeitstracking, Aufzeichnungsmöglichkeiten, Log-Files, Anzeige der Teilnehmerdaten inkl. E-Mail-Adressen etc...) sind in der DSFA als objektive Möglichkeiten zu berücksichtigen, die durch Einstellungen im Rahmen der Nutzung verändert werden.

Mit diesen **Einstellungen**, die der **Verantwortliche** selbst vornimmt, wird das **Risiko für die betroffenen Personen herabgesenkt**.

Einsatz im Unternehmen – Befassung des Betriebsrates

Wenn Mitarbeiter*Innen-Daten im Unternehmen erhoben werden, spielt die Arbeitnehmerdatenverarbeitung immer eine Rolle.

Es ist zu prüfen, ob uU eine **Betriebsvereinbarung zu Videokonferenzen** notwendig ist, weil zB Logfile-Daten anfallen, und damit eine „**Mitarbeiterüberwachung**" objektiv möglich ist.

Zu beachten ist auch, dass viele Mitarbeiter*Innen über **Teleworking** an Videokonferenzen teilnehmen werden, und uU **Privaträumlichkeiten** dann „eingesehen" werden können.

Je nachem, wie das konkrete Tool, das verwendet wird, ausgestaltet ist, und wie die Möglichkeiten der Nutzung im Unternehmen sind, bedarf es daher der Mitarbeit des Betriebsrates um die arbeitsverfassungsrechltiche Einordnung sowie Zulässigkeit herzustellen. Zu bedenken ist dabei, dass es nicht auf die konkrete Einsatzart (zB keine Aufzeichnungen, kein Aufmerksamkeitstracking) ankommt, sondern bereits die Möglichkeit derartiger Funktionen dazu führt, dass die Arbeitsleistung während einer bestimmten Tätigkeit zu irgendeinem Zweck überprüft werden kann. Es ist für die Qualifikation als technische Kontrollmaßnahme nicht nötig, dass der Dienstgeber die durch das Tool zur Verfügung gestellten Möglichkeiten auch nutzt.

In Betrieben ohne Betriebsrat bedarf der Einsatz derartiger Tools der Zustimmung der Mitarbeiter*Innen im Einzelfall nach § 10 Abs 1 AVRAG.