Checkliste für die Durchführung von Videokonferenzen
während der Kontaktbeschränkungen

Für die Durchführung von datenschutzgerechten virtuellen/Video-Konferenzen empfehle ich wie folgt vorzugehen:

A. Auswahl

Prüfen Sie,

1. ob anstelle von Videokonferenzen auch Telefonkonferenzen ausreichen könnten, um die gewünschte Abstimmung unter den Teilnehmern herbeizuführen? Diese können sehr viel leichter datenschutzgerecht durchgeführt werden.

2. ob es Ihnen mit verhältnismäßigem Aufwand möglich ist, einen eigenen Dienst mit öffentlich verfügbarer oder kommerziell erhältlicher Software bereitzustellen? Stellen Sie dabei sicher, dass die eingesetzte Software keine Daten über Ihre Beschäftigten oder deren Kommunikationspartner/-innen an den Hersteller oder Anbieter der Dienst übermittelt.

3. ob eine der Lösungen eines Anbieters mit Sitz im Europäischen Wirtschaftsraums (EWR) oder aus einem Land mit gleichwertigem Datenschutzniveau Ihren Anforderungen entspricht?[1]

Prüfen Sie des Weiteren, ob der Anbieter

a) vertrauenswürdig ist,

b) ausreichende Datensicherheit (zum Beispiel durch anerkannte Zertifizierung) nachweisen kann und

c) Ihnen die Verschlüsselung der Datenübertragung garantiert.

Fällt diese erste Prüfung positiv aus, dann

d) schließen Sie einen ordnungsgemäßen Auftragsverarbeitungsvertrag mit dem Anbieter und nehmen diese zu der Datenschutzdokumentation,

und stellen Sie sicher, dass der Betreiber

e) keine Angaben über Ihre Beschäftigten und deren Kommunikation oder über die Nutzung der Software für eigene Zwecke verarbeitet, sowie

f) Unterauftragnehmer mit Sitz außerhalb des EWR für die Bereitstellung des Videokonferenz-dienstes nur einsetzt, wenn der Datenexport die Anforderungen des Kapitel V der DSGVo erfüllt.

Bitte beachten Sie, dass der Beschluss der EU-Kommission zur Gleichwertigkeit des Datenschutzniveaus in den USA sich ausschließlich auf Organisationen erstreckt, die sich durch Selbstzertifizierung beim US-Handels-ministerium zur Einhaltung der Grundsätze des Privacy Shields verpflichtet haben. Die Zertifizierung muss sich auch auf Personaldaten (HR) erstrecken[2].

Wenn Sie statt eines Anbieters gemäß Ziff. 3 einen Anbieter mit Sitz außerhalb von EWR oder einem Land mit gleichwertigem Datenschutzniveau bzw. einen nicht im Rahmen des Privacy Shields für die Verarbeitung von Personaldaten zertifizierten Anbieter in den USA beauftragen wollen, dann erfüllen Sie die Bedingungen unter

[1] Einige deutsche Anbieter hat der Deutsche Industrie- und Handelskammertag (DIHK) unter https://www.digitales-kompetenzzentrum-kiel.de/homeoffice. html zusammengestellt (Stand 30.03.2020). Ob diese Angebote dem Datenschutz entsprechen habe ich noch nicht geprüft.

[2] Überprüfen sie dies durch Einsicht in die Liste des US-Handelsministeriums unter https://www.privacyshield.gov/list.

LBC Management Support GmbH
Geschäftsführer Lars Bosse
Gohliser Straße 6
04105 Leipzig
M +49/ 175/ 89 34 038
T +49/ 341/ 5861 9451
Skype: LarsBosse1
bosse@LBC.Management
www.LBC.Management
Konto: Sparkasse Leipzig
DE93 8605 5592 1090 0006 30
BIC: WELADE8LXXX
Steuernummer: 231.133.13393
USt-Ident.Nr.: DE 286 205 860

Ziff. 3.a) – c) und e) und schließen mit ihm zur Erfüllung der Bedingung in Ziff. 3.d) einen Vertrag gemäß der von der EU-Kommission genehmigten Standardvertragsklauseln[3]. Eine Einschränkung der Wirkung dieser Klauseln durch anderweitige Vereinbarung ist nicht zulässig.

Ich weise besonders darauf hin, dass einige verbreitet eingesetzte Anbieter die aufgeführten Bedingungen zum Stand Anfang April 2020 (noch) nicht erfüllen. Dazu gehören lt. Prüfung des Datenschutzbeauftragten des Landes Berlin die Unternehmen Microsoft, Skype Communications und Zoom Video Communications.

Diese Prüfung müssen Sie schriftlich dokumentieren. Sie kann als Datenschutzfolgenabschätzung (DSFA) gewertet werden und ist zur Datenschutzdokumentationen zu nehmen.

Nicht datenschutzgerechte Lösungen, die aufgrund der Einführung der Kontaktbeschränkungen von Ihne bisher und teilweise kurzfristig eingesetzt wurden, sollten sofort abgelöst werden.

B. Umsetzung

Ist die Auswahl nach oben genannten Kriterien auf ein Tool gefallen, sind unbedingt weitere technische und organisatorische Maßnahmen zu beachten:

- Ist das Tool in der Lage, die gesendeten Daten verschlüsselt zu übertragen?
- Können Sie die Datenschutzeinstellung innerhalb des Tools manuell anpassen? Bei vielen zur Zeit sehr beliebten Tools wie z.B. Zoom ist es notwendig, die Datenschutzeinstellungen so einzustellen, um einer möglichen unzulässigen Datenverarbeitung vorzubeugen.
- Werden übermittelte Dateien, aufgezeichnete Videomitschnitte oder Fotos nach einem festgelegten Zeitraum gelöscht?
  Achtung Aufzeichnung: Sollen Teile der Videokonferenz mitgeschnitten werden, sind alle Beteiligten darüber im Vorhinein zu informieren und ggf. deren Einwilligung einzuholen!
- Einladungen sollten nur an Personen vergeben werden, die für die behandelten Themen die nötige Freigabe haben.
- Screensharing /Gemeinsame Nutzung von Bildschirmdarstellungen: Es muss zwingend darauf geachtet werden, dass nur für die Videokonferenz relevante Informationen zu sehen sind. Das heißt: Unnötige Inhalte und (PC-)Fenster sind vorher zu schließen und einen separaten Desktop einrichten, auf dem keine Dateien oder Verknüpfungen zu sehen sind.
- Achten Sie auch auf die Umgebung, in der Sie bei der Videokonferenz sitzen! Was ist im Hintergrund der Teilnehmer zu sehen? Eine neutrale Wand oder eine Pinwand mit vertraulichen Unternehmensinfos?

Lars Bosse
Datenschutzbeauftragter & -auditor (TÜV)

[3] Die Standardvertragsklauseln unter https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32010D0087