Checkliste Videokonferenz: 21.04.2020

Datenschutzaspekte Auswahl des Tools

- Überschreitet die Nutzung den rein privaten Bereich, so findet die DSGVO Anwendung. Auch bei rein privater Nutzung ist es nicht schädlich auf einen ausreichenden Datenschutz bei der genutzten Anwendung zu achten.
- Vorüberlegungen treffen: Welche Themen werden besprochen, wie sensibel sind die Inhalte? Risiko-Abwägung. Kann der Austausch sensibler Inhalte durch entsprechende Vor-bzw. Nachbereitung reduziert werden.
- Vorüberlegung: Wer sollte teilnehmen? Wie lade ich die Teilnehmer*innen ein? Ist eine Terminvereinbarung notwendig? Via Telefon, via E-Mail - hier darauf achten, dass auch wirklich nur die Teilnehmer*innen eine Einladung erhalten. Beachten Sie das Terminunfragetools auch auf eine Datenschutzkonformität geprüft werden müssen. Muss überhaupt ein solches Tool eingesetzt werden? LDSB Bayern empfiehlt "Dudle" der TU Dresden und den "DFN Terminplaner". Beide Tools sind kostenfrei.
- Soweit ein Datenschutzbeauftragt*er vorhanden ist diese/n einbeziehen
- Die Arbeitnehmervertretung im Betriebs beteiligen z.B. Betriebsrat, § 87 Abs. 1 Nr. 6 BetrVG
- Videokonferenztools (Open-Source sowie kommerzielle Anbieter) auf datenschutzfreudliche Einstellungen prüfen und ggf. anpassen, IT und Datenschutzbeauftragte/n einbeziehen - wenn keine/r vorhanden ist prüfen, ob die Landesdatenschutzbehörden sich zur Konkreten Softwareanwendung geäußert haben. Als Beispiel für Open-Source nennt die LDSB BW Nextcloud Talk, BigBlueButton, Matrix, RocketChat, Jitsi Meet.
- Bei Dritten – also externen Dienstleistern wird ein (Auftragsverarbeitungsvertrag, Art. 28 DSGVO) notwendig. Die Anbieter bieten häufig auf Ihrer Website selbst eine Vorlagen für einen solchen Vertrag an. Ansonsten finden Sie auch Vorlagen auf den Websiten der Landesdatenschutzbehörden z.B. https://www.baden-wuerttemberg.datenschutz.de/datenschutz-in-zeiten-der-krise-handreichungen-des-lfdi-helfen-bei-auftragsverarbeitung-innerhalb-der-eu-und-des-ewr/
- Standort des Servers etc. Deutschland, EU, Drittland?
- Soweit der Standort außerhalb der EU liegt, ist prüfen ob es ich um ein sicheres Drittland handelt und ausreichend Garantien für den Datenschutz vorhanden sind (Art. 44 ff DSGVO)
- Liegt für das Drittland ein Angemessenheitsbeschluss nach Art. 45 DSGVO vor https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en
- Teilnehmer*innen/ Beschäftigte Informieren Art. 12 ff DSGVO, Betroffenenrechte, Speicher- und Löschfristen etc.
- Soweit ein Betriebsrat vorhanden ist eine Betriebsvereinbarung für Onlinekonferenzen, Softwarenutzung abschließen oder ergänzen.

Technisch-Organisatorische Maßnahmen (TOM) treffen

- Information, Sensibilisierung; Schulung der Beschäftigten, Teilnehmer*innen
- Software wählen, welche flexibel eingesetzt werden kann nach Bedarf für 10 oder 100 Teilnehmer*innen damit nicht mehrere Tools angelernt werden müssen
- Vor der Teilnahme an einer Videokonferenz ist über Verarbeitung personenbezogener Daten im Rahmen der Videokonferenzen im Sinne des Art. 13 DSGVO zu informieren. Der Hinweis kann in die E-Mail Einladung zu einem Meeting/Videokonferenz aufgenommen werden.

Maria Dimartino – Rechtsanwältin | Im Faltersgraben 4 – 69509 Mörlenbach | Tel.:06209 2722790 |
www.jurvita.de | - mail@jurvita.de

Softwareeinstellungen

- Weiterleiten von Zugangslinks ausschließen bzw. in der Einladung darauf hinweisen, dass diese Daten nicht weitergeleitet werden dürfen.
- Einladung/Konferenzlink nicht via Socialmedia/Messenger oder Videokonferenztool versenden
- Ausschluss von „Schatten-IT“ /keine Nutzung von anderen Messenger/Diensten daneben
- Herstellung einer sicheren Internetverbindung bzw. Arbeitsoberfläche (z.B. via VPN, Direct Access),
- Zutritt zur Onlinekonferenz nur via Passwort ermöglichen
- Das Passwort darf nicht in der gleichen E-Mail wie die Einladung versenden (kann z.B. zuvor telefonisch festgelegt werden)
- Virtuelles Wartezimmer aktivieren, Moderator*in lässt Teilnehmer*innen nach Prüfung (Name, E-Mail) eintreten
- Auf Verschlüsselte Übertragung achten (Ende-zu-Ende- Verschlüsselung)
- Zum Dateienaustausch eigene Cloud verwenden nicht die Funktion des Videokonferenztools
- Einstellungen ändern, dass diese datenschutzfreundlich sind (z.B. kein Aufmerksamkeitstracking, kein Profiling etc.)

Hardware

- Bereitstellung einer sicheren IT (mit aktuellen Schutzprogrammen)
- Oder BYOD (Bring your own Device - Beschäftigte nutzen ihre eigenen Geräte) nach bestimmten Vorgaben (kleinster gemeinsamer Nenner ist häufig nur das Smartphone, daher sollte das Tool auch via Smartphone bedienbar sein). Die zu installierende APP darf eine Freigabe auf die gespeicherten Kontakte im Smartphone/Tablet erhalten.

Organisatorisches

- Teilnehmer*innen sollten sich mind. 15 Minuten vorher in den Warteraum einwählen und Mikrofon und Kopfhörer testen, prüfen was in der Kamera alles sichtbar ist
- Zugewiesenes Erstpasswort ändern. Sicheres Passwort erstellen (Passwortpolicy). PW nicht automatisch speichern.
- Bestimmten Ansprechpartner benennen, wenn es während der Onlinekonferenz zu technischen Problemen kommt.
- Vorüberlegungen treffen welche Handlungen notwendig werden wenn die Technik bei a) einer Person b) oder allen ausfällt (Plan B?)
- Gibt es die Möglichkeit einer Fernwartung?
- Teilnehmer*innen nochmals verdeutlichen, dass ein grds. Aufzeichnen nicht zulässig ist und sogar eine Straftat darstellen kann.
- Klären von welchem Ort an der Videokonferenz teilgenommen werden kann (Home-Office, Während der ÖPNV Nutzung? Auch wenn technisch Möglich nicht unbedingt zu empfehlen während eines Supermarkteinkaufes)
- Sind zusätzliche Maßnahmen notwendig, wenn ein/e Teilnehmer*in im Ausland, EU-Ausland ist?
- Ausschluss von Dritten, verschlüsselte Übertragung, räumlich sich distanzieren (Home-Office) Headset, Kopfhörer nutzen, ggf. Bildschirmfolie
- Auch Mitbewohner/Familienanghörige haben nicht an einer Videokonferenz teilzunehmen/ mitzuhören (z.B. in anderen Raum gehen, Kopfhörer nutzen)
- Entfernen Sie Sprachassisstenten aus dem Raum
- Klären welche Dateien, Inhalte für eine Videokonferenz geeignet sind und welche eher nicht. Soweit vorhanden virtuelle Plattform oder Cloud nutzen um Inhalt bereits

Maria Dimartino – Rechtsanwältin | Im Faltersgraben 4 – 69509 Mörlenbach | Tel.:06209 2722790 |
www.jurvita.de | - mail@jurvita.de

vorzubereiten. Agenda und Unterlagen zur Vorbereitung vorab sicher übermitteln z.B. via Cloud/Passwort
- Was ist sichtbar, wenn ich den Bildschirm teile/freigebe? E-Mail, Chat-Programme, Kalender schließen damit nicht unbeabsichtigt Pop-up Fenster /Meldungen ins Bild geraten
- Was ist im Hintergrund sichtbar/seriösen virtuellen Hintergrund nutzen
- Bereitstellen von Dateien zur Vor- und Nachbereitung: Für die Übermittlung von Dateien (in der Regel geschlossene Dateien z.B. .jpg .pdf nutzen, es sei denn an diesen muss etwas bearbeitet werden. Soweit ein internes Tool besteht um Daten auszutauschen (Cloud/ Downloadserver) ist dieses vorzuziehen gegenüber dem Chatfenster/ Dateiübermittlungsfunktion des Videokonferenztools.

Know-How Vermittlung

- Erstellen Sie eine Anleitung als .pdf und ggf. mehrere Kurzvideos
- Vermittlung von grundlegenden technischen Know-hows
- Datenschutzkenntnisse, eine Vielzahl von Datenpannen werden durch Anwenderfehler verursacht!
- Ansprechpartner/in bei Problemen benennen, dies beugt einer sog. „Schatten-IT“ vor
- Meldung von möglichen sog. Datenpannen regeln

Beteiligungsrechte Arbeitnehmervertretungen

- Betriebsvereinbarung zur Onlinekonferenznutzung, Softwarenutzung
- Betriebsvereinbarung Home-Office, Datenschutz, IT-Nutzung, Softwarenutzung
- Versetzungen, §§ 95 Abs. 3 BetrVG, 99 BetrVG

Die Liste ist nicht abschließend und wird auch noch ergänzt.

Viel Erfolg!

Maria Dimartino

Maria Dimartino – Rechtsanwältin | Im Faltersgraben 4 – 69509 Mörlenbach | Tel.:06209 2722790 |
www.jurvita.de | - mail@jurvita.de