Datenschutz-NEWS

DRIMALSKI &Partner

…zu den aktuellen Ereignissen der letzten Wochen [12/2020]

Sicherheit und Datenschutz bei Videokonferenz-Software

14.12.2020 - Videokonferenzen datenschutzkonform durchführen (Anleitung)

[Julia Peidli; activeMind AG]

13.11.2020 - Videokonferenzen und Datenschutz: Der große Vergleichstest zu Zoom und Co.

[Rechtsanwalt Sören Siebert; eRecht24 GmbH & Co. KG]

Auch wenn die Einhaltung der DSGVO in Zeiten von Corona aus Sicht der Unternehmen nicht oberste Priorität hat, herrscht bei der Verwendung von Online-Tools kein rechtsfreier Raum. Um Ärger mit Datenschützern, Mitarbeitern, Geschäftspartnern zu vermeiden sollte sich bei der Auswahl oder Überprüfung der Videokonferenz-Lösung etwas Zeit genommen werden. Es ist nämlich damit zu rechnen, dass die Datenschutzbehörden in den nächsten Wochen und Monaten die Anbieter von Videokonferenz-Lösungen noch sehr viel stärker unter die Lupe nehmen und kontrollieren sowie ggfs. sanktionieren.

Welche Anforderungen sind bei der Auswahl und beim Einsatz von Videokonferenzsystemen wichtig?

Die Datenschutzkonferenz der Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) hat eine Orientierungshilfe[1] zu den Anforderungen für die Auswahl und beim Einsatz von Videokonferenzsystemen veröffentlicht. Die wichtigsten Punkte und Hinweise sind in nachfolgender Übersicht zusammengefasst.

✓ **Betriebsmodelle / Möglichkeiten für den Einsatz von Videokonferenzsystemen**

- **Selbst betriebener Dienst für Videokonferenzen:**
  - ➔ Vorteil: Datenerhebung und alle Datenflüsse können selbst kontrolliert werden.
- **Betrieb durch einen externen IT-Dienstleister:**
  - ➔ Besteht der Auftrag des ext. IT-Dienstleisters in der Bereitstellung und Wartung des Videokonferenzsystems und hat dieser kein eigenes Interesse an den Daten, ist ein Auftragsverarbeitungsvertrag (AVV) abzuschließen.
  - ➔ Prüfen: Gibt die durch den Dienstleister eingesetzte Software Daten an Hersteller / andere Dritte weiter?
- **Online-Dienst / Nutzung von Online-Videokonferenz-Tools:**
  - ➔ Ein entscheidendes Auswahlkriterium sind die vom Dienstleister ergriffenen technischen und organisatorischen Maßnahmen, welche vorab zu prüfen sind, ob der eingesetzte Dienstleister einen ausreichenden Schutz bietet.
  - ➔ Grundsätzlich sind Anbieter, die ihren Sitz in der EU bzw. dem EWR haben, zu bevorzugen. Da aber gerade die großen Anbieter von Videokonferenzsystemen ihren Sitz in den USA haben, ist seit dem Wegfall des EU-U.S. Privacy Shields *[wir berichteten hierüber in unseren Datenschutz-NEWS 09/2020]* darauf zu achten, dass der entsprechende Anbieter zusätzliche Garantien für die Sicherheit der Datenverarbeitung in den USA bietet. Die DSK weist explizit darauf hin, dass bei *„der Verwendung von Standardvertragsklauseln und anderen vertraglichen Garantien als Grundlage für Übermittlungen personenbezogener Daten [pb-Daten] in die USA […] nach der Entscheidung des Europäischen Gerichtshofs (EuGH) zusätzliche Maßnahmen zu ergreifen [sind], die sicherstellen, dass für diese Daten auch bei und nach ihrer Übermittlung ein im Wesentlichen gleichwertiges Schutzniveau wie das in der EU gewährleistet wird“*.

✓ **Rechtliche Anforderungen an die Nutzung von Videokonferenzen**

- **Verantwortliche ermitteln:**
  - ➔ Empfehlung: Im AVV festhalten, dass der Anbieter die pb-Daten der Teilnehmer nur auf Weisung des Verantwortlichen und nicht für eigene Zwecke verarbeiten darf (= keine gemeinsamen Verantwortlichkeit gem. Art. 26 DSGVO).

[1] 23.10.2020: https://www.datenschutzkonferenz-online.de/media/oh/20201023_oh_videokonferenzsysteme.pdf

© Drimalski & Partner GmbH 2021

- **Rechtsgrundlage bestimmen:**
  - ➔ z.B. Einwilligung in die Verarbeitung, Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses, Verarbeitung zur Wahrung der berechtigten Interessen des Verantwortlichen/Dritten (Interessenabwägung)

✓ **Technische Anforderungen an Videokonferenzen**

- **Sicherheit der Verarbeitung:**
  - ➔ Sicherheit der Daten auf dem Transportweg mittels mindestens Transportverschlüsselung.
  - ➔ Empfehlung: Zur Erhöhung der Sicherheit sind vorhandenen Zusatzfunktionen wie private Chats, Screensharing, Bereitstellung von Dokumenten in einem allen Teilnehmern offenstehenden Arbeitsbereich zu unterbinden.
- **Nutzerauthentifizierung:**
  - ➔ Bei normalen Risiken genügt eine Authentifizierung mit Nutzername und geeignetem Passwort, wohingegen bei einem hohen Risiko mindestens eine Zwei-Faktor-Authentifizierung erforderlich ist.
  - ➔ Externe Personen erhalten einen Gastzugang (keine vorherige Nutzerauthentifizierung) z.B. über einen Einladungslink. Die DSK hat folgende Bedingung für das Anbieten eines Gastzugangs aufgestellt:
    - Der Gastzugang ist für jeweiligen Anwendungsfall erforderlich.
    - Risiken für die Betroffenen, die durch eine nicht autorisierte Teilnahme entstehen, sind gering.
    - Es ist gewährleistet, dass nur Personen teilnehmen, die untereinander bekannt sind. Nicht autorisierte Personen werden erkannt und können aktiv ausgeschlossen werden, noch bevor sie aktiv der Videokonferenz teilnehmen können.
- **Installation und Softwareaktualisierung:**
  - ➔ Der Veranstalter der Videokonferenz ist dafür verantwortlich, dass das System auf dem neuesten Stand ist und alle bekannt gewordenen Sicherheitslücken beseitigt wurden.
- **Rollentrennung:**
  - ➔ Bei der Auswahl des jeweiligen Videokonferenz-Tools darauf achten, dass mindestens folgende Rollen eingerichtet werden können:
    - Administrierende: Festlegung von Parametern, Zuweisung der Moderationsrolle.
    - Moderierende: Videokonferenzen anberaumen, Personen einladen oder ausschließen, Zutritt eröffnen und schließen sowie Präsentationsrolle zuweisen.
    - Präsentierende: Medien/Dokumente für anderen Teilnehmer bereitstellen, Wortemeldungen steuern.
    - Teilnehmende: Eigenen Aufzeichnungs- und Wiedergabegeräte steuern.
  - ➔ Wichtig ist auch, dass jede Person ihre Kamera und ihr Mikrofon jederzeit deaktivieren kann.
- **Datensparsamkeit:**
  - ➔ Es dürfen nur die zur Bereitstellung des Dienstes zwingend erforderlichen technischen und sonstigen Informationen verarbeitet werden. *„Analysen des Nutzungsverhaltens und die Verarbeitung personenbezogener Diagnose- und Telemetrie-Daten durch den Anbieter des eingesetzten Dienstes zu eigenen Zwecken widersprechen dem Grundsatz der Datensparsamkeit, sofern sie nicht für die Diensterbringung erforderlich sind und eine eigene Rechtsgrundlage haben“*, so die DSK.

Die o.g. Orientierungshilfe der DSK zeigt deutlich auf, dass Videokonferenzen nicht einfach mal so eingesetzt werden sollten. Zusätzlich zur Orientierungshilfe hat die DSK eine Checkliste[2] veröffentlicht. Unternehmen sollten also zügig daran arbeiten die eingesetzten Tools für Videokonferenzen (möglichst) datenschutzkonform zu betreiben. **Einen Datenschutz-Vergleich mit Bewertung der wichtigsten Videokonferenz-Anbieter als Übersichtsliste können Sie bei uns auf Anfrage an datenschutz(at)drimalski.de erhalten.**

[2] 11.11.2020: https://www.datenschutzkonferenz-online.de/media/oh/20201111_checkliste_oh_videokonferenzsysteme.docx

© Drimalski & Partner GmbH 2021

Worauf ist bei der Inbetriebnahme und dem Einsatz einer Videokonferenz-Lösung zu achten?

Die Tools auf dem Markt bieten neben verschiedenen Tarifen und technischen Möglichkeiten auch unterschiedliche Voraussetzungen und Einstellungen zum Datenschutz. Wichtig ist, dass bestimmte datenschutzrechtliche Punkte beachtet werden:

✓ **Anbieter hat Sitz in der EU oder ein angemessenes Datenschutzniveau**
- Anbieter aus der EU sind aus Datenschutzsicht sicherer (= einheitliches Datenschutzniveau).
- Bei Anbieter aus Drittländern (EU-Ausland) auf Einhaltung angemessene Datenschutzvorschriften achten:
  - ➔ ***Angemessenheitsbeschluss der EU-Kommission***
    Für einige Ländern wurde festgestellt, dass dort das Datenschutzniveau „angemessen" (also vergleichbar mit EU) ist: Andorra, Argentinien, Färöer Inseln, Guernsey, Japan, Israel (teilweise), Kanada, Neuseeland, Schweiz.
  - ➔ ***Standard Contractual Clauses (SCC) / Standardvertragsklauseln***
    Nach SSC verpflichtet sich der Anbieter zur Wahrung des europäischen Datenschutzes.
  - ➔ ***EU-US Privacy-Shield***
    Das EU-US Privacy-Shield kann nicht mehr als Rechtsgrundlage herangezogen werden.

✓ **Datenschutzeinstellungen sind so sicher wie möglich eingestellt**
- Die Datenschutzeinstellungen sind je nach Tool verschieden. In erster Linie sollten Übertragungen ausschließlich verschlüsselt erfolgen. Die Aufzeichnungen und etwaige Chat-Protokolle sollten nach der Beendigung des Meetings auch gelöscht werden. Ein Tracking der Teilnehmer sollte nach Möglichkeit ebenfalls abgestellt werden.

✓ **Ein Auftragsverarbeitungsvertrag (AVV) wurde mit dem Anbieter abgeschlossen**
- Anbieter gelten i.d.R. als Auftragsverarbeiter. Daher muss mit diesen ein AVV abgeschlossen werden.

✓ **Der Betriebsrat (wenn vorhanden) wurde bei der Auswahl beteiligt**
- Mit dem Betriebsrat (wenn vorhanden) können Absprachen anfallen, wenn durch das Online-Konferenz-Tool Login-Daten verarbeitet werden und/oder die Teilnahme der Mitarbeiter quasi „überwacht" werden kann. Das ist nach § 87 Abs. 1 Nr. 6 BetrVG zwingend.

✓ **Die Datenschutzhinweise/-informationen wurden ergänzt**
- Bei Nutzung von Videokonferenz-Tools mit Kunden, Mitarbeiter oder Geschäftspartnern müssen diese Tools in den Datenschutzhinweisen aufgenommen werden (u.a. Tool-Name, Zwecke der Verarbeitung von Nutzerdaten, Rechtsgrundlage, Speicherdauer, Anbieter-Anschrift, Abschluss eines Vertrags zur Auftragsverarbeitung mit Anbieter).
- Bei Einladung zur Videokonferenz müssen die Teilnehmer auch über Datenschutzfragen informiert werden (am einfachsten durch einen Link auf der Anmeldeseite zur Videokonferenz oder einen Verweis in der Einladungsmail).

✓ **Das Verarbeitungsverzeichnis wurde an die Nutzung von Videokonferenz-Tools angepasst**
- Unternehmen sind nach Art. 30 DGSVO verpflichtet, ein Verzeichnis von Verarbeitungstätigkeiten zu führen. Dort sollte auch das eingesetzte Videokonferenz-Tool erwähnt werden.

Das sollte jetzt konkret getan werden:

- ✓ **Prüfen anhand o.g. Vorgaben, ob die genutzte Videokonferenz-Lösung datenschutzkonform einsetzbar ist.**
- ✓ **Prüfen, ob ein Auftragsverarbeitungsvertrag mit dem Anbieter abgeschlossen wurde.**
- ✓ **Prüfen, ob die datenschutzfreundlichsten Einstellungen im Tool gewählt wurden.**
- ✓ **Ergänzen der Datenschutzhinweise/-informationen um einen Passus zum genutzten Videokonferenz-Tool.**
- ✓ **Ergänzen des Verarbeitungsverzeichnisses nach Art. 30 DSGVO um das eingesetzte Videokonferenz-Tool.**

© Drimalski & Partner GmbH 2021