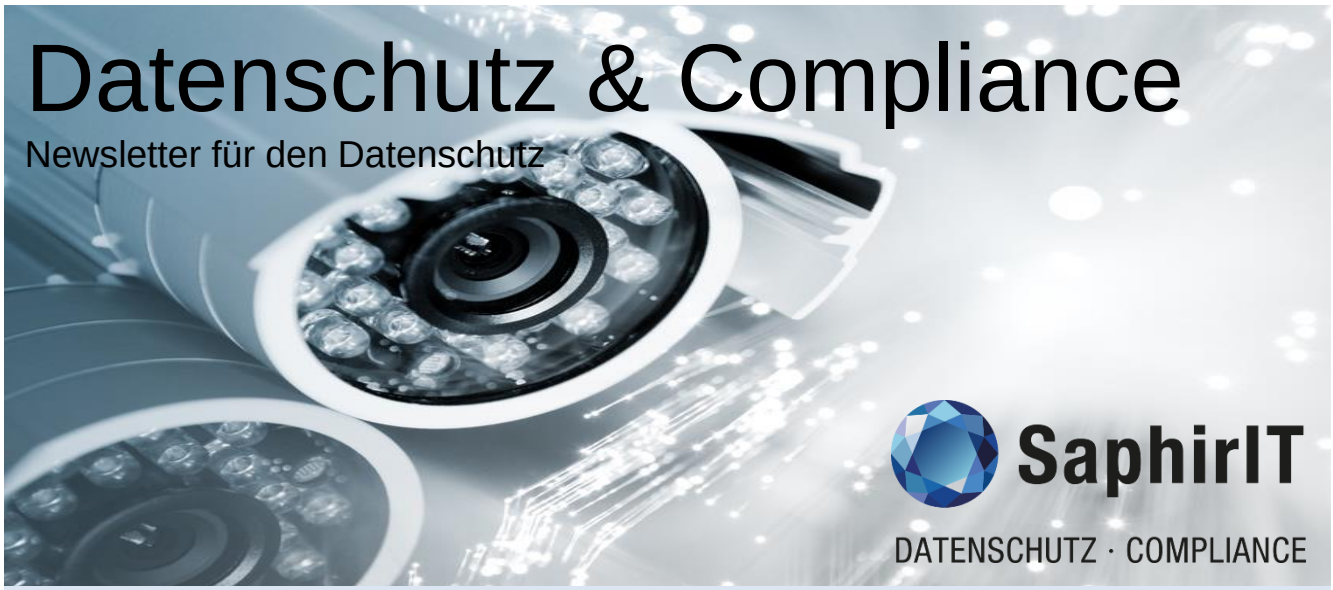

Ausgabe Mai 2020 | Seite 161 - 165

INHALT

Sehr geehrte Damen und Herren,

hiermit übersenden wir Ihnen unseren Newsletter Mai 2020.

Viel Spaß bei der Lektüre. Bei Fragen oder Anmerkungen sprechen Sie uns gerne an.

Bleiben Sie gesund!

Mit freundlichen Grüßen
Ihre SaphirIT GmbH

Datenschutzrechtliche Anforderungen an Videokonferenzprogramme

Videokonferenzlösungen werden in diesen Tagen mehr genutzt denn je. Der Einsatz von Videokonferenzprogrammen stellt dabei ein wertvolles Hilfsmittel dar. Aber nicht nur in Zeiten von Corona sollten Unternehmen bestimmte arbeits- und datenschutzrechtliche Anforderungen genau beachten.

Wir geben Ihnen in dieser Spezialausgabe einen Überblick auf was Sie bei der Auswahl eines Videokonferenzprogramms achten und welche Vorkehrungen gegebenenfalls getroffen werden müssen.

Häufig genannte Programme sind beispielsweise Skype for Business, Webex, Microsoft Teams oder Zoom. Pauschal kann bei keinem der erwähnten Programme ein komplett datenschutzkonformer Einsatz gewährleistet werden. Viele Anbieter haben ihre Server in den USA. Eine Datenübertragung ist dann häufig auf das datenschutzrechtlich sehr umstrittene Privacy

Shield gestützt. Aber auch wenn Daten innerhalb der EU gespeichert werden, müssen die Anbieter datenschutzrechtliche Vorgaben hinsichtlich beispielsweise Auskunfts- und Transparenzpflichten beachten.

Der Schutz personenbezogener Daten darf beim Einsatz eines solchen Programms nicht außer Acht gelassen werden. Die Nichteinhaltung geltender Datenschutzvorschriften kann gegebenenfalls teure Folgen haben. Datenschutzverstöße, auch bei der nicht datenschutzkonformen Verwendung von Videokonferenzprogrammen, können mit Bußgeldern von bis zu 4 % des Jahresumsatzes oder bis zu 20 Millionen Euro sanktioniert werden.

Grundsätzlich gilt, dass es einer Interessenabwägung bedarf, bevor der Einsatz eines Videokonferenzprogramms zustande kommen kann. Die betroffenen Grundrechtspositionen und widerstreitenden Interessen müssen in Ausgleich gebracht werden. Arbeitnehmerinteressen können insbesondere dann entgegenstehen, wenn das Tool zur Arbeitnehmerüberwachung (z.B. Anwesenheitskontrolle oder Aufmerksamkeitstracking) eingesetzt werden soll.

Die Landesbeauftragte für Datenschutz vom unabhängigen Landeszentrum für Datenschutz (ULD) in Schleswig-Holstein hat losgelöst von einzelnen Videokonferenzanbietern Regeln und Maßnahmen veröffentlicht.

Das ULD schildert, man solle sich zunächst die Frage stellen, ob es in der konkreten Situation überhaupt einer Videokonferenz bedürfe oder ob nicht auch eine Telefonkonferenz oder schriftliche Kommunikation ausreiche.

Ist eine Videokonferenz tatsächlich notwendig und auch gewollt, so müssen in einem nächsten Schritt datenschutzrechtliche Rahmenbedingungen geschaffen werden.

Datenschutzrechtliche Rahmenbedingungen

Wenn Sie sich als Unternehmen entscheiden einen Online-Dienst zu nutzen, müssen die spezifischen datenschutzrechtlichen Anforderungen zusammen mit der IT-Administration und der bzw. dem Datenschutzbeauftragten geklärt werden.

Ausschlaggebend hierbei können insbesondere die Datenverarbeitung innerhalb der EU, die Verwendung datenschutzfreundlicher Voreinstellungen oder der Einsatz von Verschlüsselung etc. sein.

Bereits im Vorfeld einer Videokonferenz sollten erforderliche Dokumente auf sicheren Wegen an die Teilnehmer verteilt werden. Und auch wenn es selbstverständlich sein dürfte, so sollte das Umfeld einer Videokonferenz derart gestaltet sein, dass im Hintergrund keine persönlichen oder vertraulichen Dinge sichtbar sind.

Was ist bei den Funktionalitäten zu beachten?

Der Funktionsumfang des Programms sollte sich auf das für die Kommunikation notwendige beschränken. Das Prinzip der Datenminimierung aus der Datenschutzgrundverordnung (DSGVO) ist dabei stets zu beachten.

Folgende Punkte sind besonders relevant:

1. **Trackingfunktionen**

Trackingfunktionen, um Arbeitnehmer oder deren Arbeitszeiten zu überwachen, müssen ausgeschaltet sein. Hierunter fallen einerseits die Funktion den Anwesenheits- und Aktivitätsstatus (aktiv/inaktiv/abwesend) des Arbeitnehmers zu verfolgen, andererseits das Aufmerksamkeitstracking während des Meetings oder ob das Tool lediglich im Hintergrund laufen gelassen wird.

2. **Aufzeichnung von Konferenzen**

Von einer Aufzeichnung ganzer Videokonferenzen sollte, so auch das ULD, abgesehen werden. Bei einer Aufzeichnung stellen sich immer viele weitere Fragen die dann geklärt werden müssen. Beispielsweise Zugriffsberechtigungen, Löschfristen oder auch die Gewährleistung der Betroffenenrechte. Teilnehmer einer Konferenz sollten sich generell anderweitig Notizen machen oder sich Dokumente und Präsentationen im Nachgang per E-Mail zusenden lassen

3. **Zugangsbeschränkungen**

Organisatoren eines Meetings sollten darauf achten, dass ein Passwort verwendet wird, um dem Meeting beizutreten. Des Weiteren bietet es sich an das Meeting zu schließen, wenn alle Teilnehmer anwesend sind, sodass selbst bei Kenntnis des Passworts, es anderen Unbefugten nicht möglich ist sich in das Meeting einzuwählen.

Abgesehen von diesen technischen Maßnahmen, die ein verwendetes Videokonferenzprogramm gewährleisten sollte müssen unternehmen weitere Maßnahmen treffen, wenn ein Videokonferenzprogramm im Unternehmen etabliert wird.

- **Auftragsverarbeitungsvereinbarung**

Entscheiden Sie sich als Unternehmen für ein Konferenzprogramm, so muss gemäß Art. 28 DSGVO mit dem Anbieter der Anwendung eine Auftragsverarbeitungsvereinbarung geschlossen werden. Viele Anbieter stellen eine solche Vereinbarung auf ihrer Webseite zur Verfügung. Dieser Pflicht sollte dann in jedem Fall nachgekommen werden, unabhängig vom gewählten Konferenzprogramm und ob sonstige datenschutzrechtliche Aspekte eingehalten werden

- **Datenschutzfolgenabschätzung**

Gegebenenfalls muss im Einzelfall auch eine Datenschutzfolgenabschätzung vorgenommen werden. Grundsätzlich gilt je größer der Eingriff, desto eher besteht die Pflicht eine solche vorzunehmen

- **Datenschutzinformationen**

Allen Teilnehmern einer Videokonferenz muss im Vorfeld eine Datenschutzinformation zur Verfügung gestellt werden, indem

insbesondere die Verarbeitung im Zusammenhang mit dem Einsatz des Konferenzprogramms erklärt wird

- **Verzeichnis von Verarbeitungstätigkeiten**

Auch in das bereits vorhandene Verzeichnis von Verarbeitungstätigkeiten muss ein neues Verfahren für die Konferenzen aufgenommen werden

- **Betriebsrat**

Sofern ein Betriebsrat vorhanden ist, muss dieser bei der Einführung eines Konferenztools zustimmen. Der Betriebsrat hat gemäß § 87 Abs. 1 Nr. 6 Betriebsverfassungsgesetz (BetrVG) bei der „Einführung technischer Systeme, die zur Überwachung des Verhaltens und der Leistung der Mitarbeiter bestimmt sind“ ein Mitbestimmungsrecht. Dabei ist es schon ausreichend, dass eine objektive Eignung zur Leistungs- oder Verhaltenskontrolle besteht, ohne dass von dieser tatsächlich Gebrauch gemacht wird

Fazit

Im Moment sind viele verschiedene Anbieter von Videokonferenzprogrammen auf dem Markt. Jedes Programm muss für sich datenschutzrechtlich bewertet werden. Wie bereits geschildert liegen viele Server der Anbieter (so z.B. bei Microsoft Teams oder auch Zoom) in den USA. Eine datenschutzkonforme Nutzung ist bisher nur über das datenschutzrechtlich nicht unumstrittene Privacy-Shield möglich.

Bisher werden Datenübertragungen auf Grundlage des Privacy-Shields von den Aufsichtsbehörden noch akzeptiert. Dennoch sollte nach Möglichkeit darauf verzichtet werden.

Wenn alle anderen notwendigen, oben geschilderten Maßnahmen getroffen und auch ansonsten im Unternehmen ein ordnungsgemäßer Datenschutz vorliegt halten wir, die Nutzung eines solchen Programms für akzeptabel.

Der Landesbeauftragte für Datenschutz und Informationsfreiheit Baden-Württemberg hat auf seiner Internetseite zu datenschutzfreundlichen technischen Möglichkeiten der Kommunikation Stellung genommen und dabei auch einige Lösungen aus verschieden Bereichen aufgezählt (vgl. https://www.baden-wuerttemberg.datenschutz.de/datenschutzfreundliche-technische-moeglichkeiten-der-kommunikation/).

Vorbehaltlich einer umfassenden Prüfung schlägt der Landesbeauftragte Baden-Württemberg Lösungen aus verschiedenen Bereichen vor.

Dazu zählen:

- Nextcloud Talk
- BigBlueButton
- Matrix
- RocketChat
- Jitsi Meet

Bevor aber auch auf eine dieser Lösungen zurückgegriffen wird, sollte eine umfassende datenschutzrechtliche Prüfung durchgeführt werden.

Sollten Sie Fragen zu einem der Programme haben sprechen Sie uns gerne an.

Hinweis: Der Bundesdatenschutzbeauftragte Ulrich Kelber hat ganz aktuell vor der Nutzung des Anbieters Zoom gewarnt. Es gäbe derzeit keine Ende-zu-Ende-Verschlüsselung, was heiße, dass die Inhalte der Kommunikation unverschlüsselt auf den Server des Anbieters lägen.

Er rate von der Nutzung dringend ab, wenn personenbezogene Daten im Spiel sind. Es sollte dann bestenfalls eine andere Plattform gewählt werden, auf der eine Ende-zu-Ende-Verschlüsselung garantiert sei.

Kelber führt weiter aus: „Ich erwarte von Behörden und großen Firmen, aber auch von Bürgerinnen und Bürgern, genau hinzusehen, wofür sie sich entscheiden.“ Es gebe immer eine Alternative, „die die Vertraulichkeit der Kommunikation sichert und deren Nutzung man nicht mit seinen Daten oder Metadaten bezahlt“.

SaphirIT GmbH
Sutthauser Straße 285
49080 Osnabrück
Geschäftsführer
Amtsgericht Osnabrück

www.saphirit.de
USt-ID-Nr. DE268765300
Frank W. Stroot
HRB 20385

Oldenburgische Landesbank AG
IBAN DE29 2802 0050 5042 8200 00
BIC OLBODEH2XXX

Telefon 0541/60079296
Telefax 0541/60079297
datenschutz@saphirit.de