Datenschutzfreundliche technische Möglichkeiten der Kommunikation

Gepostet von Pressestelle | 17. April 2020 | Aktuelle Meldungen, Datenschutz

Angesichts der aktuellen Situation um COVID-19 stehen datenschutzrechtlich Verantwortliche vor der Aufgabe, technische Möglichkeiten der Online-Kommunikation einzuführen oder auszuweiten. Hierbei stellen sich auch einige Herausforderungen bei der Einhaltung geltender Datenschutzgesetze.

Bei der Auswahl von Video- oder Telefonkonferenzsystemen sollte aus technischer Sicht darauf geachtet werden, dass der Anbieter

KONTAKT

Telefon
0711 / 61 55 41 – 0
Montag bis Freitag von 10 bis 12 Uhr.

E-Mail
poststelle@lfdi.bwl.de

DE-Mail
poststelle@lfdi.bwl.de-mail.de

ACHTUNG: *Nur für Versand von Nachrichten über das DE-Mail-System, nicht für normale E-Mails!*

Hinweis zum E-Mail-Versand
Wir empfehlen, vor dem Senden von E-Mail-Nachrichten die angehängten Dokumente in die neuen Formate (z.B. docx / xlsx / pptx) oder in „pdf“ umzuwandeln.

Bitte klicken Sie hier für weitere Kontaktmöglic

weder Metadaten (wer hat wann mit wem kommuniziert) noch die Inhaltsdaten der Kommunikation für eigene Zwecke auswertet oder an Dritte weitergibt. Dies können datenschutzrechtlich Verantwortliche am besten sicherstellen, wenn sie oder ihr Dienstleister (im öffentlichen Bereich sind das z.B. BITBW bei Landesbehörden oder Komm.ONE bei Kommunen) eine entsprechende Softwarelösung „On Premises“ – also im eigenen Rechenzentrum – bereitstellen oder aufbauen. Dadurch ist es möglich, alle Datenflüsse und Datenerhebungen selbst zu kontrollieren. Dazu bieten sich zahlreiche Lösungen auf Basis von Open-Source-Software an (z.B. Nextcloud Talk, BigBlueButton oder Matrix), die prinzipiell datenschutzgerecht einsetzbar sind.

Details

Bei der Verarbeitung personenbezogener Daten haben Verantwortliche die allgemeinen Anforderungen der DS-GVO einzuhalten. Insbesondere ist bei der Auswahl von Kommunikationslösungen im speziellen darauf zu achten, dass die Verantwortlichkeit, ggf. gemeinsame Verantwortlichkeit, geklärt ist und nötige Verträge geschlossen werden, Datenverarbeitung (auch von Analyse-, Telemetrie- und Diagnosedaten) nur aufgrund und im Rahmen einer Rechtsgrundlage stattfindet, die Datenverarbeitung fair und transparent ist und Übermittlungen in das Ausland außerhalb des EWR nur unter den besonderen einschlägigen Voraussetzungen stattfindet. Hierzu sollten sich Verantwortliche vorab einen Überblick über Vertragsverhältnisse und Datenflüsse (Zwecke, übertragene Daten, Empfänger) verschaffen.

Häufig sind Anwendungen datenschutzfreundlicher, die selbst betrieben werden können („On Premises“), beispielsweise auf eigenen Servern oder mit Hilfe von Dienstleistern mit Auftragsverarbeitungsverträgen. Der Vorteil ist, dass dort personenbezogene Daten wie Metadaten (wer hat wann mit wem kommuniziert) oder Inhaltsdaten der Kommunikation (z.B. Videobild, Screensharing) grundsätzlich nicht an Dritte übertragen werden. Zu den möglichen selbst

hkeiten.

betriebenen, von uns nicht im Detail geprüften, Lösungen aus verschiedenen Bereichen zählen beispielsweise:

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

Trotz der Verwendung selbst betriebener Kommunikationslösungen kann es sein, dass Hersteller beim Betrieb der Software personenbezogene Daten erheben (insbesondere Analyse-, Telemetrie- und Diagnosedaten), z.B. durch die Einbindung von Tracking-Pixeln in Webseiten oder einer serverseitigen Übermittlung von personenbezogenen Daten an den Hersteller, mit weiterer Verarbeitung für eigene Zwecke. Stichproben haben ergeben, dass Apps für mobile Endgeräte neben der Kommunikation mit der selbst gehosteten Anwendung auch eine Kommunikation mit dem Hersteller der App oder mit Dritten durchführen. Daten werden dann sowohl vom Anwender als Betreiber des Servers als auch vom Hersteller der App und von Dritten verarbeitet. Beispielsweise überträgt die iOS-App Jitsi-Meet neben der Übertragung von Videosignalen auch Daten an den Hersteller und dessen Auftragsverarbeiter.

Es empfiehlt sich, Nutzern den Hinweis zu geben, wie eine App möglichst datensparsam eingesetzt werden kann (z.B. Deaktivierung der Erhebung von Statistikdaten oder Absturzberichten). Dieses insbesondere deshalb, weil wir bei einer ersten kursorischen Prüfung von verschiedenen Apps Datenübertragungen festgestellt haben, bei denen Verantwortlicher, Zweck, Datenkategorien und Rechtsgrundlage unklar bleiben. In Datenschutzhinweisen ist teilweise auch zu lesen, dass Daten für eigene Zwecke erhoben werden, die nicht für die Diensterbringung erforderlich sind,

sondern u.a. für die Produktentwicklung genutzt werden. Oftmals erheben die Web-Versionen von Videokonferenz-Diensten weniger Daten als Desktop-Anwendungen oder Smartphone-Apps.

Ein weiteres Kriterium bei der Auswahl einer datenschutzfreundlichen Lösung ist auch, ob personenbezogene Daten außerhalb des Europäischen Wirtschaftsraums verarbeitet werden. Neben der technischen Umsetzung ist bezogen auf die konkreten Datenflüsse auf die Erstellung von Datenschutzhinweisen nach Art. 13 DS-GVO und den Abschluss ggf. datenschutzrechtlich notwendiger Verträge zu achten.

Ein datenschutzkonformer und sicherer Betrieb einer Kommunikationslösung kann nur durch entsprechende technische und organisatorische Maßnahmen erreicht werden. Dazu zählen unter anderem:

- Alle Datenflüsse sind per Transportverschlüsselung (TLS) nach dem Stand der Technik abzusichern. Dies schützt vor dem Mitschneiden durch unbeteiligte Dritte auf dem Transportweg.
- Bei sensiblen Daten oder wenn ein nicht 100% vertrauenswürdiger Dienstleister verwendet wird, sollte der Inhalt zusätzlich per Ende-zu-Ende-Verschlüsselung (E2EE) geschützt sein.

Beim Durchführen einer Videokonferenz sollte die Aufzeichnung von Sprache und Video deaktiviert sein und nur bei Vorliegen einer Rechtsgrundlage aktiviert werden und in diesem Fall eine aktive Aufzeichnung allen Teilnehmern signalisiert werden. Auf die Strafbarkeit des unbefugten Abhörens oder Aufzeichnens des nichtöffentlich gesprochenen Wortes (§ 201 StGB) wird hingewiesen. Funktionen, welche die Aktivität von Nutzern überwachen, erfordern ebenfalls eine gesonderte Rechtsgrundlage und Transparenz. Aus unserer Sicht sollte Teilnehmern die Möglichkeit angeboten werden, auch ohne aktive Videokamera an einer Konferenz

teilzunehmen, gerade dann, wenn diese aus ihrer Privatwohnung heraus erfolgt.

Weitere Hinweise für die Auswahl von Videokonferenz-Systemen finden Sie z.B. in

- den Empfehlungen und der Checkliste für Videokonferenzsysteme der Berliner Beauftragten für Datenschutz und Informationsfreiheit,
- im Kompendium Videokonferenzsysteme des BSI,
- oder in der Praxishilfe Videokonferenzen und Datenschutz der Gesellschaft für Datenschutz und Datensicherheit (GDD e.V.).

Grundsätzlich ist die Frage zu stellen, ob Videokonferenzen überhaupt immer das richtige Werkzeug sind. Diese sind generell sehr ressourcenaufwendig und störungsanfällig. Daher sollten Videokonferenzen nur dann genutzt werden, wenn es wirklich notwendig ist, zum Beispiel wenn Präsentationen mit einer Bildschirmfreigabe gehalten werden sollen. Oftmals kann es je nach Kontext und Erfahrung der Teilnehmer sinnvoller sein, einen Großteil der Kommunikation per Text, E-Mail (ggf. verschlüsselt), Chat oder Audio-Konferenz abzuwickeln. Bei vielen Videokonferenzlösungen ist die Anzahl an maximalen Teilnehmern begrenzt oder sie sind technisch nicht praktikabel. Abseits von der Praktibilität von Videokonferenzen gilt es insbesondere im Schulbereich zu prüfen, ob die mit einer Videokonferenz verbundene zusätzliche Übertragung personenbezogener Daten (aktuelles Aussehen, persönliche Dinge im Hintergrund) zur Zweckerreichung erforderlich ist.

Eine objektive Übersicht und bereitgestellte Funktionen von Videokonferenzlösungen ist hier zu finden: https://en.wikipedia.org/wiki/Comparison_of_web_conferencing_software. Bei der Übersicht ist jedoch zu beachten: Eine datenschutzrechtliche Einschätzung oder eine Beurteilung der Anwenderfreundlichkeit ist nicht Bestandteil dieser Tabelle auf Wikipedia.

Nachfolgende Alternativen können anstatt oder als Ergänzung zu Videokonferenzen genutzt werden:

- Telefon- oder Audiokonferenzen
- Datenschutzfreundliche und sichere Messenger
- E-Mail, ggf. per Ende-zu-Ende-Verschlüsselung gesichert
- Text-Chats über datenschutzfreundliche und Ende-zu-Ende-verschlüsselte Plattformen
- Einfache Werkzeuge zur gleichzeitigen Bearbeitung von Textdokumenten wie Etherpad oder komplexere Werkzeuge wie Cryptpad oder Nextcloud

AKTIE:

‹ VORHERIGER

Corona im Rechtsstaat

NÄCHSTER ›

Virtuelle Konferenz über Zoom: Online-Schulstunde an Freiburger Gymnasium gehackt