Overview - Data Protection & IT Security issues regarding video conferencing systems

Osborne Clarke

Bundesverband Deutscher Stiftungen

13 May 2020

Ulrich Bäumer & Oliver Rohn

Introduction

Bundesverband Deutscher Stiftungen

- Many companies and also consumers now use different video conference services
- This presentation shall serve as an overview about some of the most popular video conference service providers and shall give you an idea which applications, systems or platforms can (or should not) be used for a specific purpose
- This overview is not exhaustive and we do not make recommendations for individual offers as the requirements vary

Overview

1. Microsoft Teams
2. Skype for Business
3. Cisco Webex
4. Google Meet
5. GoToMeeting
6. Zoom
7. Eyeson
8. Wire
9. BlueJeans
10. Jitsi Meet

1. Microsoft Teams

Microsoft Teams ("**MS Teams**") is an application that allows groups of people to come together into a shared digital space to communicate and collaborate in real time with one another. These groups are called 'Teams' and can be set up to limit access to only those people that shall be included.

Once included in a 'Team', members can engage in continuous, social media style conversation with one another. It also allows those people to collaborate on documentation, where real-time amendments can be made and seen by multiple people at the same time. MS Teams is also the long term replacement for Skype for Business.

As a Microsoft product, MS Teams is subject to the company's privacy policy (https://privacy.microsoft.com/en-GB/privacystatement). Amongst others, the following data is collected:

- **Environmental information** such as device and operating system versions, regional and language settings, counters for sign-in attempts and failures; **Usage data** such as number of calls made, number of IMs sent or received, number of meetings joined, frequency of features used, and stability issues; **Error report data** such as information about performance and reliability, device configuration, network connection quality, error codes, error logs, and exceptions.

1. Microsoft Teams

- MS Teams uses cookies and web beacons to save and maintain the user's preferences and settings.
- According to the MS Security Framework for Teams, **all traffic (server-to-server or client-to-server) is encrypted.**
- MS Teams enables to create and manage own meeting policies to control the features available to participants. Furthermore, additional resources such as the MS Trust Center are offered to team administrators. The MS Trust Center provides information on how MS Teams implements the GDPR: https://www.microsoft.com/en-gb/trust-center/privacy/gdpr-overview.
- It is also possible to increase data security of a conference via general team settings. For example: Control access to team meetings, control whether anonymous persons can participate in meetings or define which chats can be used. A summary of the setting options according to safety relevance can be found at: https://sharepoint360.de/13-tipps-um-microsoft-teams-sicher-zu-machen-und-datenschutz-zu-gewaehrleisten/.

2. Skype for Business

- Microsoft Skype for Business ("**Skype**") provides instant messaging (IM), audio and video calls, online meetings, availability (presence) information, and sharing capabilities all from one program. As a Microsoft product, Skype for business is subject to the company's privacy policy (like MS Teams).

- As with MS Teams, Skype uses cookies or other technologies and, according to the Skype for Business Framework, the communication is encrypted.

- In a guideline on its website, Microsoft refers to most security issues while using Skype for business ("Security and Skype for business"). Users and/or administrators thus receive an overview which security tools are used and how data is encrypted. As with MS Teams, the MS Trust Center is also available to users and administrators of Skype.

- **As far as we know, there are no current discussions concerning a lack of IT security or data protection measures when making use of Skype.**

3. Cisco Webex

- Cisco Webex Meetings ("**Webex**") is a cloud collaboration platform for video conferencing, online meetings, screen share, and webinars. Due to the Coronavirus, Cisco announced that it extends its offer to use Webex for free.

- On the website, users are informed comprehensively about the processing of their personal data in terms of Art. 13 GDPR. Moreover, the Webex website offers comprehensive guidance on the GDPR implementation. The privacy policy can be accessed through the following link: https://www.cisco.com/c/de_de/about/legal/privacy-full.html

- Webex collects personal data such as **name, address, email address, phone number, login information (account number, password), marketing preferences, social media account information, or payment card number**. Webex further collects personal data from trusted third-party sources and engage third parties to collect personal data to assist.

- Webex shares personal data with third parties for the purpose of operating the business, delivering, improving, and customizing the solutions. In case third parties use personal data, Webex claims that all purposes are permitted by applicable law.

3. Cisco Webex

- Webex makes use of automatic data collection tools such as cookies, embedded web links, and web beacons. These tools collect certain standard information (e.g. IP-address, browser type, clickstream behaviour).

- According to its website, Webex offers a comprehensive end-to-end encryption. All information is encrypted while in use and before it leaves the device, not just in transit and in rest. Also search queries are encrypted.

- Limited access: Only authenticated users can view messages and files in Webex Teams spaces. Additionally, Webex provides guidance on how to use such service securely: https://help.webex.com/de-de/8zi8tq/Cisco-Webex-Best-Practices-for-Secure-Meetings-Hosts

- In recent years (2017 – 2019), Webex had to face criticism due to certain security gaps. However, they were able to fix the gaps shortly after and further provided security advisories. **As far as we know, there are no publications or discussions on recent IT security or data protection issues concerning the use of Webex.**

4. Google Meet

- Tech giant Google offers three different communication tools: Google Hangouts, Duo and Meet. While Hangouts and Duo could rather be compared to FaceTime calls or video calls via WhatsApp, Google Meet is aimed primarily at teams who want to hold video conferences.

- With the expansion of Google Meet, Google is now abandoning the previous brand name Hangouts for its video chat products. In the long term, Google Meet will therefore become the video chat tool of Google.

- Google Meet was previously reserved for paying business customers with a G Suite subscription. Now, Google has changed its mind: starting as of 4 May 2020, the software is to be made available to all users step by step free of charge.

- Google Meet employs an array of counter-abuse protections to keep the user's meetings safe. These include anti-hijacking measures for both web meetings and dial-ins.

- Google informs its users ecompassingly about the security of their personal data, accessible under the following link: https://support.google.com/a/answer/7582940?hl=de.

4. Google Meet

- To limit the attack surface and eliminate the need to push out frequent security patches, Google Meet works entirely in the user's browser. This means Google does not require or ask for plugins or software to be installed if Chrome, Firefox, Safari, or Microsoft Edge are used. For mobile use, they recommend installing the Google Meet app.

- To help ensure that only authorized users administer and access Google Meet services, they support multiple 2-step verification options for accounts that are secure and convenient. Additionally, Google Meet users can enroll their account in Google's Advanced Protection Program (APP), which provides strong protections against phishing and account hijacking and is specifically designed for the highest-risk accounts.

- In Google Meet, all data is encrypted in transit by default between the client and Google for video meetings on a web browser, on Android and iOS apps and in meeting rooms with Google meeting room hardware.

- **As far as we know, there are no current discussions concerning a lack of IT security or data protection measures when making use of Google Meet.**

5. GoToMeeting

The web-based GoToMeeting service by LogMeIn Inc. provides a platform for conventional video transmissions and screen transmissions to a wide audience and can support multiple monitors. The transmission can be limited to one application window. Meetings can also be recorded and saved for later viewing.

Pursuant to the Privacy Policy, GoToMeeting collects the following information from users:

- Customer Account and Registration Data: Information provided to create account or register for events, webinars, surveys, etc. such as first and last name, billing information, password and email address
- Service Data: Information either voluntarily entered by the user or others (for example, schedules, attendee info, etc.), or passively logged by the website or Service itself, (for example, duration of session, use of webcams, connection information, etc.), usage and log data about how the services are accessed and used, including information about the used devices to access the Services, IP addresses, location information, language settings, operating system, unique device identifiers and other diagnostic data
- Third Party Data: Information from other sources, including publicly available databases or from third parties
- Location and device information.

5. GoToMeeting

- GoToMeeting uses several analytical tools, inter alia Google Analytics.
- On the website, users are informed about the processing of their personal data in terms of Art 13 GDPR. The privacy policy can be accessed through the following link: https://www.logmeininc.com/legal/privacy
- GoToMeeting uses very strong SSL encryption on their website. This technology uses strong passwords, login information and activity logging and performs regular audits of network security controls in order to prevent security breaches. Moreover, additional internal password protection has been developed which gives users certain access but keeps them from accessing meeting rooms or areas that need to be separate.
- **As far as we know, there are no current discussions concerning a lack of IT security or data protection measures when making use of GoToMeeting.**

6. Zoom

Zoom ("**Zoom**") has recently been faced with criticism due to its lack of **IT security and inconsistent data protection** precautions, which boils down in particular to the following issues:

- Cyber attackers made use of the rise in Zoom usage to target people with the intention of capturing and stealing personal information. If teleconferences are not set to private, they can be accessed by strangers, provided they somehow receive the link to the conference meeting.

- Moreover, data is not always transferred fully encrypted. The encryption only works reliably as long as everyone in a conference is using zoom software. If someone dials in by phone, the encryption of the service does not work.

- Administrators of a conference can also use the service to view data such as the IP address, location and information about the hardware used and were further able to control which conference participants have the app in the foreground and which are busy with other things.

- The service's iOS app sent some information about the device used **to Facebook**, such as model, free space and display size. The privacy policy did not contain any indication that data had been passed on to Facebook.

6. Zoom

After Zoom's IT security and data protection measures have been criticised massively, Zoom just announced that it has closed several security gaps.

- In a blogpost dated 1 April 2020, Eric S. Yuan, the founder and CEO of Zoom, announced details about the measures they implemented recently and the ones that they are going to address which can be accessed through the following link: https://blog.zoom.us/wordpress/2020/04/01/a-message-to-our-users/.

- Inter alia, Zoom removed the attendee attention tracker feature.

- Further, Zoom announced that they took action to remove the Facebook Software Development Kit in their iOS client and reconfigured it to prevent it from collecting unnecessary device information from users.

- Class action against Zoom: In California, US, Zoom has been sued under a class action by one of its shareholders on Tuesday, 31 March 2020. Zoom is accused to overstating its privacy standards and failing to disclose that its service **was not end-to-end encrypted**. The Shareholder claimed in a court filing that a string of recent media reports highlighting the privacy flaws have led to the company's stock, which had rallied for several days in the beginning of the year, to plummet. They have lost nearly a third of their market value since touching record highs in late-March.

7. Eyeson

Eyeson GmbH is an Austrian startup and supplies integrated cloud-based video conferencing solutions. Due to the Covid-19 crisis, Exoscale, the European cloud of A1 Digital, and Eyeson are cooperating to offer their customers "**all eyes(on) Exoscale**", a videoconferencing solution via click & talk. Until 30 June 2020, customers can set up digital meetings for their companies free of charge.

- The **hosting** is carried out **exclusively in European data centres** - and can be used easily via web-based access. All eyes (on) Exoscale runs on the European cloud platform Exoscale in a data center in Germany (Munich and Frankfurt), in Austria in Vienna or Switzerland (Geneva and Zurich), depending on the customer's location.

- Information about how Eyeson processes personal data can be viewed here: https://www.eyeson.com/privacy-policy/

- Eyeson uses cookies, beacons, scripts and tags to analyse trends, administer the website and gather demographic information about its user base and uses web push notifications to retarget visitors if allowed in the notification preferences.

7. Eyeson

- In particular, Eyeson addresses customers working in sensitive sectors such as the healthcare, education and legal sector.

- Pursuant to further information on its website, Eyeson is compliant with the GDPR. Eyeson informs its users in detail about its commitment to data privacy which can be accessed through the following link: https://intercom.help/eyeson-room/en/articles/1939016-eu-gdpr.

- **As far as we know, there are no current discussions concerning a lack of IT security or data protection measures when making use of Eyeson.**

8. Wire

Wire Swiss GmbH ("**Wire**") offers a wide range of features - from one-on-one to group conversations, temporary messaging, voice and video conferencing, screen and file sharing. Wire is listed on the Internet as "Whats-App Messenger alternative". With its versions **Wire Pro** and **Wire Red**, it is primarily intended to address companies. These versions offer administration possibilities for teams and video conferences with several participants.

- According to information on its website, Wire stores only such data needed to synchronize conversations between a user's devices, to detect fraud and spam and to resolve customer issues. Among others, this includes information to create the user account such as name, email address or mobile phone number and technical information (such as the type of device users authorized for the Wire application) to pass data between endpoints.

- Wire offers comprehensive security and privacy whitepapers to give an overview of collected data, metadata and technical information. These documents are available under https://wire.com/de/security/.

8. Wire

- For business prospects and accounts, Wire may use Marketo, Salesforce, Clearbit, Calendly, DocuSign and Stripe to send out emails, for management of the customer relationship, to schedule product demos and to ensure the billing of the service.

- According to its privacy policy and security whitepaper, all communication is secured by end-to-end encryption. Wire also uses transport encryption to protect metadata.

- Wire is committed to working with independent security experts to publish regular audits of various components of its applications.

- Wire is compliant with the GDPR and supports customers in complying with the requirements of the GDPR.

- **As far as we know, there are no current discussions concerning a lack of IT security or data protection measures when making use of Wire. Even the German Government has confidence in Wire and is currently testing its usage in a pilot project.**

9. BlueJeans

- Blue Jeans Network, Inc.'s videoconferencing service "BlueJeans" is a cloud-based conferencing service and provides a cost-effective, scalable solution on a robust distributed architecture.

- **BlueJeans provides conference room security as follows**: Randomly selected nine-digit meeting IDs; meeting PIN code option; option of mandatory encryption for participants; manual lock option for meetings; alarm for unsecured end points.

- BlueJeans just published general recommendations to ensure the security of video conferences.

- It focuses specifically on spontaneous connections via an app or the browser (without download). In addition, the BlueJeans meeting solution also supports conference systems (depending on the subscription plan) and can be embedded in business applications such as Microsoft Teams or Slack.

- BlueJeans informs its users very detailed about the processing of their personal data (https://www.bluejeans.com/privacy-policy).

- **As far as we know, there are no current discussions concerning a lack of IT security or data protection measures when making use of BlueJeans.**

10. Jitsi Meet

- Jitsi Meet is a free video conferencing software that works with open source code. 8×8, Inc. is the main contributor to this solution.

- Users do not need to create an account to hold videoconferences. They just need to open the program in their web browser and create a conference room. All other participants are invited via link - without having to register. Jitsi Meet can also be used via Android and iOS.

- The chat messages are end-to-end encrypted. The group video chat, however, is not. Here, data is only encrypted for transport, but briefly decrypted on the server over which the service is running. Therefore, theoretically it is possible that third parties are listening in on this.

- The privacy policy does not inform the users adequately in accordance with the requirements of the GDPR.

- **Huge advantage:** Can be quickly installed on an own dedicated server.

- **As far as we know, there are no current discussions concerning a lack of IT security or data protection measures when making use of Jitsi Meet.**

Questions?

Bundesverband Deutscher Stiftungen

Thank you

Ulrich Bäumer, LL.M. (Washington, DC)
Partner / Rechtsanwalt

Attorney-at Law (N.Y)

E: Ulrich.Baeumer@osborneclarke.com

M: +49160/96936939

Oliver Rohn
Justiziar/

Rechtsanwalt (Syndikusrechtsanwalt)

E: oliver.rohn@stiftungen.org

T: +49 30 30 89 79 47-52