Annex to the CCBE Guidance on the use of remote working tools by lawyers and remote court proceedings

Analyses of videoconferencing tools

This document is an annex to the CCBE guidance on the use of remote working tools by lawyers and remote court proceedings. It presents the individual research papers that were prepared by the CCBE examining the terms and conditions of a number of frequently used platforms, in order to compare them and to gain an understanding of the practical issues which arise in relation to legal practice.

Due to the fast development of this field, it needs to be stressed that the papers herein contained the papers may not reflect the changes introduced by providers after the research was conducted.

TABLE OF CONTENTS

Microsoft Teams

1. Who is the data controller?

The data controller is, in principle, the law firm, in our case CMS. The GDPR requires the controller to conclude a DPA with Microsoft when using Teams. Microsoft offers a standard template for this purpose.

However, the Berlin Data Protection Officer was the first supervisory authority that has determined that MS Teams does not fulfil the requirements of the GDPR and has issued on 3 July 2020 the following statement on MS Teams (with a summary right at the beginning in bold letters) (translated with Deepl):

Microsoft Teams (as part of Microsoft 365 under validity of the Online Service Terms)

Provider reserves the right to process order data for its own purposes. Defects in the order processing contract. Many ambiguities and contradictions in the order processing contract. Illegal data exports. Provider has made extensive subsequent changes to published order processing contract without identification; version (according to metadata) dated 3.1.2020 contains inadmissible restrictions on the right to issue instructions.

Important note: Microsoft has made extensive subsequent changes to the "Appendix to the Privacy Policy for Microsoft Online Services (German, January 2020)" (hereinafter: "DPA") without marking it. There is a document that was created on 3.1.2020 according to the meta-information and a document that was created on 9.6.2020 according to the meta-information. The names of the documents are the same, the document published by Microsoft on the Internet has been tacitly replaced. In the history of changes ("Clarifications and summary of changes") it is explicitly stated "None", even though large parts of the contract were changed. Most of these changes are of a purely linguistic nature. In particular, in the version of 9.6.2020, the annex Standard Contractual Clauses, which originally contained very extensive deviations from the wording of the approved standard contractual clauses, was essentially adapted to the approved text. However, there are also relevant changes in content. Most of the changes are positive. Nevertheless, one of the most important basic problems of the contract, that it is unclear and contradictory in many places, remains.

Microsoft reserves the right in the DPA to process personal data that is actually processed on behalf of Microsoft for its own purposes under the heading "Data Protection Provisions - Nature of Data Processing; Ownership". There is no apparent legal basis for the disclosure of personal data by the person responsible to Microsoft. From the processing of the order data also for Microsoft's own purposes, the problem of joint responsibility under Art. 26 DS-GVO follows. According to the case law of the European Court of Justice, such a joint responsibility is obvious, but cannot be ruled out in any case on the basis of the only rudimentary information in the DPA. This is a problem at least with regard to accountability (Art. 5(2) in conjunction with Art. 5(1)(a) GDPR). In the case of actual existence, there is also the fact that there is no agreement under Art. 26 GDPR.

In many places, the DPA contains provisions which contradict the minimum legal requirements. In the section "Data Protection Provisions - Processing of Personal Data; DPA", however, there is an unclear reference to Annex 3 to the DPA, which in turn reproduces essential content from Articles 28, 32 and 33 GDPR, but also leaves it unclear whether these rules should or should not take precedence over the actual - clearly illegal - text of the DPA. The file version of 9.6.2020 even worsens this clause by now referring to "[the] personal data of the GDPR". Such an unclear contract processing agreement makes it impossible for those responsible to fulfil their accountability under Article 5 (2) in conjunction with Article 5 (1) lit. a GDPR.

However, Annex 3 to the DPA (in the file version of 3.1.2020) also does not completely adopt the relevant wording of Art. 28 GDPR. In any case, No. 2 lit. g of Annex 3 (in the file version of 3.1.2020) falls short of the minimum legal requirements of Art. 28 (3) lit. g GDPR in that deletion or return of the order data after the end of the order is only envisaged at the customer's request and not in every case. Point 2 lit. a of Annex 3 (in the file version of 3.1.2020) also inadmissibly restricts the customer's right to issue instructions contrary to Art. 28 (3) lit. a GDPR, because exceptions are provided for not only on the basis of Union law or the law of the Member States to which Microsoft is subject. In the file version of 9.6.2020, these defects were tacitly eliminated, just as the wording of the Annex was further approximated to the wording of the Act. However, the wording of the law from the version dated 3.1.2020 has also been partially replaced by its own terms in the version dated 9.6.2020. In addition, a new deviation from the minimum requirements of Art. 28 (3) lit. a GDPR was introduced by excluding the obligation to notify the customer if Microsoft is obliged to process data in breach of instructions, not only on the basis of the law applicable to the processing obligation, but on the basis of any law (wording "the legislation"). A further deviation to the detriment of the customer in the new version of 9.6.2020 from No. 7 of Annex 3 is that Microsoft is not obliged to notify the customer of a so-called (instead of to the extent that, i.e. now only if the condition for all information is fulfilled and no longer, as previously, in part if the condition for parts of the information is fulfilled) this information is available to Microsoft at its reasonable discretion (instead of the objective wording "in a reasonable manner", i.e. now based on an equitable decision of Microsoft which is only subject to limited judicial review). Furthermore, it is not apparent and, due to the concealed amendment of the contract by Microsoft, not to be expected that this new version of the contract has also been agreed with existing customers.

The DPA provides for restrictions of the standard contract clauses under the item "Data security - verification of compliance". These are referred to as "Addendum to Clause 5, Paragraph f and Clause 12, Paragraph 2 of the Standard Contractual Clauses" and it is claimed that the Standard Contractual Clauses are not amended by this. It is true that there is a general statement in the introduction to the DPA that the Standard Contractual Clauses take precedence over the DPA, just as the Standard Contractual Clauses themselves, with their prohibition of amendment, contain a corresponding priority rule. It is already questionable - and problematic with regard to Art. 5 (2) DS-BER - whether the general priority clause in the introduction to the DPA is applicable in general if the concrete restriction of the standard contractual clauses in question itself claims not to constitute a restriction, so that under this assumption the priority clause cannot be applied logically. However, this can be left open, because any restriction of the rights and obligations arising from the standard contractual clauses, regardless of its wording and even if it is declared

subordinate and therefore not applicable elsewhere, leads to an inadmissible modification of the standard contractual clauses. This is because it is intended, and as a result regularly achieved, that the standard contractual clauses cannot be fully applied. Accordingly, Recital 109 of the DS Block Exemption Regulation also emphasises that other contractual clauses may not directly or indirectly contradict the standard data protection clauses. Thus, despite its presumed invalidity under civil law, the present restriction "add-on" clause also leads to an inadmissible modification of the standard contractual clauses so that they cannot justify the export of data. Although Microsoft has additionally subjected itself to self-certification in accordance with the Privacy Shield, this only applies to the USA. However, Microsoft reserves the right to process Order Data at any location where Microsoft or its sub-processors are located (DPA, section "Privacy Policy - Data Transfers and Storage Location - Data Transfers").

We would like to point out that in view of the subsequent undocumented change to the published contract processing agreement by Microsoft, we intend, in the course of audits, to also check compliance with the form of the contract processing agreement in accordance with Art. 28 Para. 9 GDPR and the corresponding verifiability (Art. 5 Para. 2 GDPR).

Further, in Germany the BRAO (the code on the conduct of lawyers) requires the law form to conclude a written service agreement with Microsoft; without such service agreement the use of Microsoft teams for client-related data would be illegal in Germany.

The DPA of July 2020 is **attached** hereto.

The criticism of the Berlin Data Protection Officer is very similar to the first two key findings in the paper of the European Data Protection Supervisor (EDPS) dated 2 July 2020 on its investigation into the EU institutions' use of Microsoft products and services (bold letters by me):

First, the licensing agreement between Microsoft and the EU institutions allowed Microsoft to define and change the parameters of its processing activities carried out on behalf of EU institutions and contractual data protection obligations. ***The discretion that Microsoft had, amounted to a broad right for Microsoft to act as a controller****. Given the EU institutions' role as public service institutions, the EDPS did not consider this appropriate. The EDPS recommended to EU institutions that they act to retain controllership.*

Second, EU institutions needed to put in place a comprehensive and compliant controller-processor agreement and documented instructions of the EU institutions to the processors. ***Their lack of control over which sub-processors Microsoft used and lack of meaningful audit rights also presented significant issues****. The EDPS made recommendations on how to improve the controller-processor agreement and put robust audit checks in place.*

The working group "Administration" of the conference of Germany's data protection authorities takes up this criticism and evaluates Office 365 as not compliant with data protection laws. It has adopted the following decision on 15 July 2020 (translated by DeepL):

Facts

The Working Group Administration of the Conference of the Independent Data Protection Authorities of the Federal Government and the Federal States (AK Verwaltung der Konferenz der unabhängigen Datenschutzhaufsichtsbehörden des Bundes und der Länder) has examined the Online Service Terms (OST) on which the use of the product Microsoft Office 365 is based as well as the Data Processing Addendum (DPA) for Microsoft online services - both as of January 2020 - and evaluated them with regard to their compliance with the requirements of Article 28 (3) of the Basic Data Protection Regulation (GDPR). It comes to the conclusion that on the basis of these documents, it was not possible to use Microsoft Office 365 in accordance with data protection regulations, at least as of January 2020. On this basis, DSK will enter into dialogue with Microsoft to solve the problems identified.
The consequences of the ECJ ruling C-311/18 (Schrems II) are not yet considered in this paper.

Evaluation of the Working Group Administration:

1.) Type and purpose of processing, type of personal data
Also taking into account the classification of the MS Office 365 service as a cloud specific service, according to which it may be appropriate to define the types of personal data and their processing purpose in general terms, it must nevertheless be possible for the client to describe both in more detail and, if necessary, to specify them in more concrete terms.
This applies in particular to the description of personal data with regard to the separate data protection requirements and risk levels, e.g. in the case of data pursuant to Art. 9 of the GDPR, as well as the purposes relevant to the client.
The processing contract must make it clear in which environment (specialized procedures) the data processing is taking place, and for which purposes the data are to be processed. In this context Microsoft is recommended to reduce the degree of abstraction and to use free fields which can be adapted if necessary. If necessary, this may even allow for a concrete designation in individual cases.

2.) Microsoft's own responsibility in the context of processing for legitimate business purposes
Microsoft's Data Processing Agreement (DPA) states that to the extent that Microsoft uses or otherwise processes personal information in connection with Microsoft's legitimate business activities, it is as an independent data controller responsible for the use and for compliance with all applicable laws and the controller's obligations.
Although a list of these legitimate business activities is provided, it is still not clear what other personal data is processed in this context. This concerns in particular the processing of personal data relating to the activities of Microsoft under points 3), 4), 5) and 6) of the definition of "legitimate business".
In addition, there is no legal basis for the transfer of other personal data from the data controller to Microsoft, e.g. in the context of telemetry, other than the contract for processing orders.
Insofar as data controllers could demonstrate a legitimate interest within the meaning of Article 6 (1) (f) of the GDPR for the transfer to Microsoft as an independent controller for the processing of data from the data controller and third parties for "legitimate business purposes", this does not apply, pursuant to Article 6 (1) sentence

2 of the GDPR, to processing carried out by public authorities in the performance of their duties. A separate legal basis is therefore required which allows public authorities to make data on employees or citizens available for these purposes.
The respective regulations on the permissibility of the processing of personal data by public authorities (in accordance with Art. 6 (3) (b) GDPR) can only be used as a legal basis to a limited extent due to the strict necessity principle (because of the relevance to fundamental rights). Only under the condition that, for example, a sustainably secure use of the software is only possible if the provider can process certain personal system data, can the corresponding data processing also be necessary for the fulfilment of the tasks.
Anyway, for public places therefore not all use cases of the "legitimate business purposes" are represented.

3.) Disclosure of processed data - Cloud Act
In the data protection regulations for Microsoft online services, Microsoft refers to the fact that processed data can also be disclosed outside the instruction of the customer if the data protection regulations provide for it or if this is required by law.
This description is not sufficiently concrete and does not determine the rights to be contractually defined by the customer. The exception may only refer to the law of the Union or national law of a member state, whereby it is not excluded that legal assistance agreements concluded by the Union or individual member states with third countries also apply to this law.
The concrete implementation and the effects of the Cloud Act, to which Micro-soft, as a US manufacturer, is subject, on the data protection issue of the legally permissible transfer of personal data in this context, have not been conclusively clarified. This assessment must also be made in the light of recent ECJ case law, which declares the Privacy Shield to be ineffective and generally questions data transfers to the USA, see ECJ, July 16, 2020 - C-311/18 "Schrems II".
Microsoft also used standard contract clauses to accompany the Privacy Shield certification. These too are to be reassessed on the basis of the latest ECJ case law.

4.) Implementation of technical and organizational measures in accordance with Art. 32 GDPR
On the part of the Conference of Federal and State Data Protection Supervisors, there is a consensus that the client must be able to review the implementation and description of the technical and organizational measures by the online service terms, the data protection regulations and other documentation provided by Microsoft and obtain sufficient (additional) information. Although a corresponding IT security guideline is mentioned in the DPA (not in the OST), it is not available before conclusion of the contract.
It should therefore be noted that Microsoft's standard EAST does not provide an adequate description of the measures offered by the online service for processing personal data that are appropriate to the risk. Microsoft's policy is that the responsible party is solely responsible for independently determining whether the technical and organizational measures for a particular online service meet its requirements, including its security obligations under applicable privacy laws. The current descriptions of the technical and organizational measures in the contract documents alone are not sufficient for the data controller (and are also difficult for the data controller to check) to make an objective assessment of whether the measures are appropriate to the risk.

5.) Deletion and return of personal data

Microsoft differentiates within the scope of processing between customer data arising from the contractual relationship and data that is processed independently for the purpose of providing "professional services" and processing for "legitimate business purposes".

In accordance with its role as "controller", Microsoft will not delete data processed for its own purposes.

Although it is understandable that this data is not part of the order processing according to the definition and is therefore processed on a different legal basis, it is nevertheless questionable how long the data is kept for own purposes. Microsoft does not comment on this.

6.) Information about subcontractors

With regard to the transfer of personal data to subcontractors, the "prior written consent of the customer to subcontract the processing of customer data and personal data by Microsoft" is only sufficient if a list of subcontractors approved by the responsible party (customer / principal) at the time of signing the contract processing agreement is included (see also 3.2.7 of Opinion 14/2019 of the European Data Protection Committee).

The "mechanism for notifying the customer of this update" provided for informing the customer about the involvement or replacement of subcontractors by subscribing to push notifications must be used proactively by Microsoft accordingly.

On 2 October 2020, the Conference of the Independent Data Protection Supervisory Authorities of the Federal Government and the States (Data Protection Conference) has supported the evaluation of its working group "Administration" on the data processing by Microsoft Office 365 of 15 July 2020 with a majority of 9 over 8 members. There is a great number of supervisory authorities who do not share the working group's view.

Therefore, the data protection supervisory authorities of Baden-Württemberg, Bavaria, Hesse and Saarland released the following press statement on 2 October 2020 (translated by DeepL):

The Conference of the Independent Data Protection Supervisory Authorities of the Federal Government and the States (Data Protection Conference) has taken note of the evaluation of its working group Administration for Order Processing at Microsoft Office 365 of 15 July 2020 by a majority of its members. The working group had examined "the Online Service Terms (OST) on which the use of the product Microsoft Office 365 is based as well as the data protection regulations for Microsoft online services (Data Processing Addendum / DPA) - both as of January 2020". The paper comes to the conclusion that on the basis of the above-mentioned documents, it is not possible to use Microsoft Office 365 in accordance with data protection regulations.

The decision of the data protection conference was made by a narrow majority of 9 votes with 8 votes against. The state commissioners for data protection of Baden-Württemberg, Bavaria, Hesse and Saarland and the president of the Bavarian State Office for Data Protection Supervision, which is responsible for Microsoft Deutschland GmbH, were among those who spoke out against the unqualified approval.

The data protection supervisory authorities of Baden-Württemberg, Bavaria, Hesse and Saarland make it clear that they too see considerable potential for improvement in Microsoft Office 365 in terms of data protection law, particularly in view of the recent decision of the European Court of Justice on international data transfers of 16 July 2020 (C-311/18 - Schrems II). They therefore support the objectives of the working group in principle, in so far as it formulates starting points for improvements to the Microsoft Office 365 product in terms of data protection law. However, they cannot share its overall assessment because it is too undifferentiated. Moreover, the Working Group Administration has based its assessment on contractual provisions, which Microsoft has already revised twice in the meantime. Finally, it has not yet been possible to take into account the findings of the European Court of Justice on the requirements of the basic data protection regulation for international data transfers.

Against this background, the data protection supervisory authorities of Baden-Württemberg, Bavaria, Hesse and Saarland have considered the evaluation of the Working Group Administration of July 15, 2020 as a relevant working basis, but not yet ready for decision. This is all the more true since Microsoft has not yet been formally heard on the assessments of the Working Group on Administration, as is part of a fair, constitutional process.

The five data protection supervisory authorities are all the more pleased that the Data Protection Conference has unanimously set up a working group which, under the leadership of the State Commissioner for Data Protection of Brandenburg and the Bavarian State Office for Data Protection Supervision, is to begin talks with the manufacturer in the near future.
Dr. Stefan Brink, Prof. Dr. Thomas Petri, Michael Will, Prof. Dr. Michael Ronellenfitsch and Monika Grethel: "We agree with the entire data protection conference that the legal uncertainties in the data protection handling of Microsoft Office 365 must be resolved in a timely manner. It would be a good thing if the newly appointed working group of the conference, while respecting the principles of the rule of law, could ensure that the manufacturer will soon make lasting improvements to its Microsoft Office 365 product in terms of data protection law. In a constructive dialogue with Microsoft, the standards to be observed in the case of transfers from third countries according to the latest case law of the European Court of Justice must be discussed.

2. Where is the data stored?

The place of data storage depends on the location of the data controller. You find the location here https://docs.microsoft.com/en-us/office365/enterprise/o365-data-locations by clicking on the country of the data controller on the right side of the page and then look for the line “Microsoft Teams”.

For Germany the Teams-data is stored in Germany: https://docs.microsoft.com/en-us/office365/enterprise/o365-data-locations#germany

However, the EDPS issued this criticism:

Third, EU institutions faced a number of linked issues concerning data location, international transfers and the risk of unlawful disclosure of data. ***They were unable to control the location of a large portion of the data processed by Microsoft. Nor did they properly control what was transferred out of the EU/EEA and how.*** *There was also a lack of proper safeguards to protect data that left the EU/EEA. EU institutions also had few guarantees at their disposal to defend their privileges and immunities and ensure that Microsoft would only disclose personal data insofar as permitted by EU law. The EDPS made recommendations to assist EU institutions in addressing these issues.*

Unless Microsoft would be entitled to unilaterally change the location of data, which should be excluded by the mandatory individual service agreement to be concluded between the German law firm and Microsoft, it appears that at least for the use of Microsoft Teams in Germany there is not issue regarding the data location. In other countries this might be different.

3. What are the most important aspects in the terms and conditions of the platform?

Microsoft provides end-to-end encryption of all data.

Further, Microsoft offers a huge number of possible security settings which make it quite challenging especially for small law firms to find the right settings.

The terms and conditions for Microsoft Teams (and most other Microsoft products) is easily found via Google here: https://www.microsoft.com/en/servicesagreement/. The Privacy Statement is included as a link right at the beginning of the terms and conditions and can be found here: https://privacy.microsoft.com/en-us/privacystatement. The DPA (as attached) is much more difficult to find – you have to access this site https://www.microsoftvolumelicensing.com/DocumentSearch.aspx and enter the words “DPA” in the search field in order to find it.

In this context, the EDPS is criticising a lack of transparency:

The abundance of contractual documents, the overlapping and conflicting terms within them, the lack of a clear order of precedence and the monthly updates to terms make it, at the very least, difficult for EU institutions, bodies, offices and agencies to discharge their information obligations to data subjects, as required by Article 4(1)(a) of Regulation (EU) 2018/1725.

Further it should be noted that in the English language version the rules on warranties and liability (which are very much drafted in favour of Microsoft) are not in compliance with German law on general terms and conditions and are therefore, at least for German customers, invalid. The German version is different and takes into account the German rules on general terms and conditions, but some of the rules nevertheless appear to be in breach of German law and are most likely invalid.

4. To what extent do the platform providers sell or share personal data?

No indication has been found that Microsoft sells customer data or other personal data related to its customers.

In the event of searches by public authorities, under German law Microsoft would only have to lay open such data that would be accessible to the authorities if it was stored locally. Additionally, if the data is stored outside of Germany, the public authority needs to file a formal request in the country in which the data is located, which often takes very long to be granted. It could be said, therefore, that the data is safer in the cloud than if stored locally in the law firm.

5. **To what surveillance might data held by the platform providers potentially be exposed?**

Since the data is end-to-end encrypted, surveillance would be challenging. Even when obliged under the US Cloud Act to lay open data to US authorities, the end-to-end encryption might make it difficult for Microsoft to obey.

6. How is the availability of remedies and competent jurisdiction?

While the English language version does not contain any rules on the competent jurisdiction for customers in the EU, in the German language version (translated with Deepl) this is the case:

"***10. company concluding the contract, choice of law and place of jurisdiction.*** *If you live in Europe (or have your principal place of business there as a company) and use free or paid services, Microsoft Ireland Operations Limited, One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, Ireland (registered with the Companies Registration Office in Ireland under number 256796 and VAT number IE 8256796 U and address 70 Sir John Rogerson's Quay, Dublin 2, Ireland) is the contracting company. The laws of Ireland shall apply to all claims relating to free and paid services. This is without prejudice to your rights under the Consumer Protection Act of the country in which we provide the Services to you and in which you are ordinarily resident (or as a company, your principal place of business). You and Microsoft agree to submit to the jurisdiction of the courts of the country in which we provide the Services to you and in which you are habitually resident (or, as a business, your principal place of business) for all disputes arising out of or relating to these Terms. Alternatively, you may choose the competent court in Ireland.*"

BlueJeans

1. Who is the data controller?

The only reference that can be found in the Terms and Conditions regarding the data controller is in Number 4 (User data, content and recording)
"To the extent that User Data provided or disclosed by Customer (as *data controller* or data exporter) is deemed "personal data" under applicable European Union law or regulation, (a) Customer agrees that BlueJeans may transfer to, store and process User Data in the United States and/or another country outside the European Economic Area where BlueJeans uses facilities in connection with the Services in order to provide the Services and support the Services and (b) BlueJeans shall (i) comply with Customer's reasonable, lawful instructions relating to the security and confidentiality of the User Data, and will maintain administrative, physical, and technical safeguards intended to protect the security and integrity of the User Data and (ii) process the User Data only in accordance with Customer's lawful instructions or the lawful instructions of the data subject."

2. Where is the data stored?

BlueJeans' Data Centers are located in California (where its headquarters are also situated), Virginia, Amsterdam (for Europe), Sydney and Singapore. However, for European citizens, data may be stored outside the EEA (see below an extract of the Privacy Policy)

> "If you are an EU resident:
> Your information may be transferred to, and stored at, a destination outside the European Economic Area ("EEA") that may not be subject to equivalent data protection law. It may be processed by staff situated outside the EEA who work for us or for one of our suppliers.
> We may transfer your personal information outside the EEA:
- In order to store it.
- In order to enable us to provide services to and fulfill our contract with you or the company your work for or the company that provides you access to the Services. This includes order fulfillment, processing of payment details, and the provision of support services.
- Where we are legally required to do so.
- In order to facilitate the operation of our group of businesses, where it is in our legitimate interests and we have concluded these are not overridden by your rights.
- Where we have your consent to do so.

> When we share information about you within BlueJeans and with third parties in countries with local laws which may differ from yours, we make use of standard contractual data protection clauses, which have been

approved by the European Commission, and we rely on the EU-U.S. Privacy Shield Framework to safeguard the transfer of information we collect from the European Economic Area to the United States. In some cases we may use other appropriate legal mechanisms to safeguard the transfer.

Where your information is transferred outside the EEA, we will take all steps reasonably necessary to ensure that your data is subject to appropriate safeguards, such as relying on a recognized legal adequacy mechanism, and that it is treated securely and in accordance with this privacy policy."

Only the most basic customer data is stored in the BlueJeans database, including: username, password (SHA-256 salted hash), email, name, title, company, and profile picture. While scheduling and conducting meetings, certain call detail records (start date/time, duration, etc.) are collected and stored for reporting.

Recordings are stored in secure containers in the cloud. These videos are encrypted at rest (AES-256bit) and are only accessible to the recording originator.

Billing Details: The BlueJeans Service currently leverages a third-party, PCI-compliant partner to handle all billing aspects of the service. This means no user credit card or billing information resides in the BlueJeans database. Because the service is used by thousands of companies globally, BlueJeans is also compliant with the EU-U.S. Privacy Shield Framework

3. **What are the most important aspects in the terms and conditions of the platform?**

4. USER DATA, CONTENT AND RECORDING

4.1 **User Data**. In order to set up accounts and use the Services, Customer may provide information, such as IP address, username, password, and personally identifiable information (e.g., name, phone number, email address, etc.) ("User Data"). Customer grants BlueJeans and its subcontractors the right to store, process and retrieve User Data in connection with providing and supporting the Services. Customer warrants that it has obtained required consent from Customer's Users to transfer User Data to BlueJeans and to process the User Data as contemplated by the Services, and agrees that BlueJeans may transfer to, store and process User Data where BlueJeans uses facilities in connection with the Services in order to provide the Services and support the Services. To the extent that User Data provided or disclosed by Customer (as data controller or data exporter) is deemed "personal data" under applicable European Union law or regulation, (a) Customer agrees that BlueJeans may transfer to, store and process User Data in the United States and/or another country outside the European Economic Area where BlueJeans uses facilities in connection with the

Services in order to provide the Services and support the Services and (b) BlueJeans shall (i) comply with Customer's reasonable, lawful instructions relating to the security and confidentiality of the User Data, and will maintain administrative, physical, and technical safeguards intended to protect the security and integrity of the User Data and (ii) process the User Data only in accordance with Customer's lawful instructions or the lawful instructions of the data subject. If BlueJeans cannot comply with Section 4.1(b), Customer's sole and exclusive remedy shall be to terminate this Agreement and cease using the Services.

4.2 **Content**. Users may display, upload and store files, recordings, sound, music, graphics and images in connection with Customer's use of the Service ("Content"). Customer represents and warrants that it owns, or has the necessary permissions to use and authorize the use of Customer's Content. Customer grants BlueJeans and its subcontractors a non-exclusive, worldwide, royalty-free, paid-up, transferable right and license to host, cache, copy, store and display Customer's Content for the purpose of and in conjunction with providing and supporting the Service. Customer acknowledges and agrees that, except as expressly set forth herein, (a) BlueJeans is not responsible in any manner for Customer's Content, (b) Customer assumes all risk associated with its Content and the transmission of its Content and (c) Customer has sole responsibility for the accuracy, quality, legality, and appropriateness of its Content.

4.3 **Recording**. The Service may provide a function that allows Users to record individual Meetings. Customer has the option to enable or disable the recording function. Customer is solely responsible for complying with all laws in any relevant jurisdiction when using this feature. BlueJeans has implemented technical and organizational measures designed to secure any Meetings that Customer records and stores from accidental loss and from unauthorized access, use, alteration or disclosure. However, BlueJeans cannot guarantee that unauthorized third parties will not be able to defeat those measures. Customer acknowledges that it stores such information at Customer's own risk.

11. **GOVERNING LAW AND JURISDICTION**. This Agreement, and any legal claim, suit, action or proceeding arising out of this Agreement, whether sounding in contract, tort or otherwise, shall be governed by and construed in accordance with the internal laws of the State of New York without giving effect to any choice or conflict of law provisions or rules in any jurisdiction. Each party irrevocably submits to the exclusive jurisdiction of the federal courts of the United States or the courts of the State of New York, and waives any objection based on improper venue or forum non conveniens.

4. To what extent do the platform providers sell or share personal data?

See below an extract of BlueJeans' Privacy Policy:

"There are certain circumstances in which we may share your information with certain third-parties. Any access by a third party to the information is managed

by BlueJeans, and the third parties are vetted based in part on their ability to protect information. International movement of information consistent with this sharing is discussed in the “How We Move Information” section below.

As part of your use of the Service, you may share information with other users of the Service. Those users of the Service may be located in nearly any location around the world, may be communicating with Third Party Sites (as defined below) while using the Services, and may be limited by law or by an agreement with us about their use of information you share. However, this Policy only addresses our use of the information.

We may share information with employees, contractors, agents, or consultants with a strict need-to-know under appropriate confidentiality obligations.

- We may share information with third parties which provide business-related functions on behalf of BlueJeans, including:
    - our business partners, customers, suppliers, service providers, vendors, and sub-contractors for the performance of any contract we enter into or other dealings we have in the normal course of business with you or the company that you work for or the company that provides you access to the Services. Some examples of such business-related functions for which we may share information may include data hosting, analyzing data, providing marketing assistance, providing customer service and technical support, processing orders, sending communications to you on our behalf or at our direction, user engagement and onboarding, soliciting feedback regarding the Services, facilitating invoicing and/or payments, and others in our reasonable discretion;
    - our auditors, legal advisors and other professional advisors or service providers;
    - credit reference agencies for the purpose of assessing your credit score where this is in the context of us entering into a contract with you or the person that you work for;
    - We may share information with our authorized distributors and resellers if you have purchased your license to the Services through a party other than BlueJeans to enable those distributors and resellers to fulfill their business obligations to you; and
    - We may share information obtained via our Services with analytics and search engine providers that assist us in the improvement and optimization of our site and subject to the cookie section of this policy.

When we employ another company to perform services of this nature, we only provide such company the right to use such information that is reasonably necessary to perform their specific function.

We may share information with other third parties, including when you provide consent for a specific situation. If BlueJeans intends on sharing any information in a manner other than as described above using any personal data in any manner that is not compatible with this Privacy Policy, and we do not have a legal basis for sharing that information without your consent, you will be informed of

such anticipated use and be given an opportunity to provide your consent for such use.

We may share information with third parties if we reasonably believe that such action is necessary to:

- comply with a legal obligation, regulation, or government request,
- enforce our policies and agreements,
- protect and defend the rights, property, and safety of BlueJeans, our customers, users, resellers, or others, or
- act in urgent circumstances to protect the personal safety of users of the Services or the public.

This includes exchanging information with other companies and organizations for the purposes of fraud protection and credit risk reduction and to prevent cybercrime.

We may share information with our subsidiaries and corporate affiliates who support our processing of personal data under this Policy.

As we develop our business, we might sell or buy businesses or assets. In the event of a corporate sale, acquisition, merger, reorganization, dissolution or similar event, information may be part of the transferred assets. You will be notified via email and/or other means with any news of a transaction and any choices you may have regarding your information.

For purposes of the California Consumer Privacy Act, we do not "sell" your personal information."

5. To what surveillance might data held by the platform providers potentially be exposed?

n.a.

For further information:

- BlueJeans Terms & Conditions: https://www.bluejeans.com/terms-and-conditions
- BlueJeans Privacy Policy: https://www.bluejeans.com/privacy-policy
- BlueJeans Network Security and Privacy: https://www.bluejeans.com/sites/default/files/pdf/Blue-Jeans-Network-Security.pdf

Cisco Terms and Conditions

Terms and Conditions:

Clicking the “Terms and Conditions” link on the Cisco home page takes one to the Website terms and conditions. In order to access the terms and conditions relevant to the Cisco Webex meeting platform,one has to go first to the product home page. The applicable conditions are found in the **Cisco Universal Cloud Agreement** (26th April, 2020) read along with **Online Privacy Statement** (1st May, 2020). Further searching of the site leads to a series of **Privacy Data Sheets** which “supplement the Cisco Privacy Statement and describe the Personal Data that Cisco collects and processes as part of the delivery of the Cloud Service to You.” as well as **Privacy Data Maps.** This provides a high degree of transparency. A pdf of the Webex Privacy data Sheet is produced herewith.

1. Who is the data controller?

Plainly, the collection and processing of data by Cisco will render it a data controller, though it is possible to conceive of circumstances where Cisco may be a processor only. Both situations are reflected in the sections “Access to and Accuracy of Your Personal Information” in the privacy Policy.

More specifically, the Webex Privacy data sheet makes clear that for user generated content, the data controller is the customer:

> If you are a user and your employer is the Customer that acquired the Service, your employer serves as the “data controller” for user generated content (see the Webex Meetings Privacy Data Map for a visualization of who is doing what with data). The information described in the table below and in this Privacy Data Sheet is accessible to your employer and is subject to your employer's policies regarding access, use, monitoring, deletion, preservation, and export of information associated with the Service.

No individual Data Protection officer is named, but, in the Privacy policy under “how to contact us” the following address is given:

EMEAR Privacy Officer
Cisco Systems, Inc.
Haarlerbergweg 13-19,
1101 CH Amsterdam-Zuidoost,
Netherlands

Under “Complain Resolution” there appears the following Note:

“Cisco’s main establishment in the EU is in the Netherlands. As such, our EU lead authority is the Dutch Autoritiet Persoonsgegevens.”

For persons resident in Europe (excluding Italy), Middle East, Africa, Asia (excluding Japan and China), Oceania (excluding Australia), the Law of the Contract is English Law and exclusive jurisdiction is conferred on the English Courts. For persons resident in Italy, Italian Law applies and exclusive jurisdiction is conferred on the Court of Milan. For unresolved privacy concerns, there is provided a link in the Privacy Statement to a free “U.S.-based third party dispute resolution provider “. Clicking on the link opens up an online Complaint Form. In certain cases binding arbitration is also available.

2. Where is the data stored?

The Universal Cloud Agreement states at section 4(d):

> Cisco may process and store Customer Data and Personal Data outside of the country where it was collected. Cisco will only transfer Personal Data consistent with applicable law. To the extent Cisco processes any Personal Data from the European Economic Area or Switzerland on Your behalf, we will do so in a manner consistent with the relevant EU- or Swiss-US Privacy Shield Principles or successor frameworks (“Principles”)

The Privacy Statement provides:

> **International Transfer, Processing and Storage of Personal Information**
>
> As Cisco is a global organization, we may transfer your personal information to Cisco in the United States of America, to any Cisco subsidiary worldwide, or to third parties and business partners as described above that are located in various countries around the world. By using our websites and Solutions or providing any personal information to us, where applicable law permits, you acknowledge and accept the transfer, processing, and storage of such information outside of your country of residence where data protection standards may be different.
>
> Cisco safeguards and enables the global transfer of personal information in a number of ways:
> ...
>
> **EU, UK and Swiss-US Privacy Shields**
>
> Cisco Systems Inc. and its US-based subsidiaries... participate in and have certified compliance with the EU-US and Swiss-US Privacy Shield Frameworks and Principles as set forth by the US Department of Commerce regarding the collection, use, and retention of personal information transferred from the European Union (EU), the United Kingdom (UK), and Switzerland, respectively. Cisco-US is committed to subjecting all personal information received from

European Union (EU) member countries, the UK, and Switzerland, in reliance on the EU-US and Swiss-US Privacy Shield Frameworks, to the Frameworks' applicable Principles. If there is any conflict between the terms in this Privacy Statement and the Privacy Shield Principles, the Privacy Shield Principles shall govern...

Cisco-US is responsible for the processing of personal information it receives, under these Privacy Shield Frameworks, and subsequently transfers to a third party acting as an agent on its behalf. Cisco-US complies with the Privacy Shield Principles for all onward transfers of personal information from the EU, the UK, and Switzerland, including the onward transfer liability provisions. In certain situations, Cisco-US may be required to disclose personal information in response to lawful requests by public authorities, including to meet national security or law enforcement requirements.

With respect to personal information received or transferred pursuant to these Privacy Shield Frameworks, Cisco-US is subject to the regulatory enforcement powers of the US Federal Trade Commission.

Cisco also relies on the EU Binding Corporate Rules provisions.

3. What data is collected?

This is particularised in the detailed tables set out in the Webex Privacy data Map, tabulated against the purpose of processing/legitimate interest. Reference is made to the pdf.

4. To what extent does Zoom sell or share personal data?

The Privacy data p map discloses no selling of Personal data.

However, any personal data held by Cisco will be susceptible to recovery under the Cloud Act and other US long arm provisions.

5. How technically secure is the platform?

Webex provides encryption in transit as standard, but offers end to end encryption as an additional option.

Jitsi

1. WHO IS THE DATA CONTROLLER?

The "Jitsy Meet Security & Privacy" note refers the user to the Privacy Supplement of 8x8 and the meet.jit.si Terms of Service
In accordance with the above, 8×8 is the main contributor to the Jitsi.org open-source video meetings solution. Meet.jit.si is an application of the Jitsi.org open-source video meetings solution that 8×8 hosts, which allows users to hold free video meetings. 8×8, Inc. ("8×8") is a Delaware corporation located at 675 Creekside Way, Campbell, California 95008, United States.

2. WHERE IS THE DATA STORED?

As per the "Jitsy Meet Security & Privacy" note, by default Jitsi Meet does not require users to create accounts. Any information users choose to enter, such as their name or email address is purely optional and is only shared with other meeting participants. Jitsi does not retain this information after the meeting.
Other pieces of data such as the chat, or speaker stats, for example, are stored for the duration of the meeting and then destroyed when it ends.
Many of these things can be customized by the configuration of the actual deployment that the user is using. Jitsi/8x8 preserve all of the above defaults but the user is strongly advised to also check out the meet.jit.si Privacy Policy and Terms of Service.
Recordings are kept on meet.ji.si servers until upload to the place indicated by the user (currently Dropbox). If meet.ji.si haven't managed to do that in 24 hours they still delete them and they are gone forever.

3. What are the most important aspects in the terms and conditions of the platform?

I. 8x8 retains personal information they collect from users where they have an ongoing legitimate business need to do so (for example, to provide users with a service they have requested or to comply with applicable legal, tax or accounting requirements). When they have no ongoing legitimate business need to process personal information, they will either delete or anonymize it or, if this is not possible (for example, because personal information has been stored in backup archives), then they will securely store personal information and isolate it from any further processing until deletion is possible.
II. According to the Privacy Notice of 8x8, EU Individuals have rights to access their stored Personal Data and to limit its use and disclosure. With Privacy Shield certification, 8x8 has committed to respect those rights. Because 8x8 Inc. personnel have limited ability to access data customers or other data controllers transmit, receive, or store through our services, if the user is an EU Individual covered by Privacy Shield and 8x8 Privacy Notice, and they wish to request access to or to limit use or disclosure of their

Personal Data, they should provide the name of the 8x8 Inc. customer or other data controller who transmitted, received, or stored Personal Data through 8x8 services. 8x8 will refer user's request to that customer or other data controller and will support that business as needed in responding to user's request.

III. Meet.jit.si uses Analytics such as Amplitude, Datadog and Crashlytics to cover various aspects of the apps and the infrastructure on meet.jit.si. Things tracked in analytics include, an anonymous identifier (users can run in "incognito" mode if this bothers them), bitrate, available bandwidth, SDP offers and answers, product utilization events, mobile app crash dumps (how much various product features are used overall). Once the meeting is over, they do not retain any names, e-mail addresses or profile pictures (those are only transmitted to the other participants in the meeting).

IV. 8x8 warns that personal information may be transferred to, and processed in, countries other than the country of residency of the user. These countries may have data protection laws that are different to the laws of the user's country (and, in some cases, may not be as protective). Specifically, their Websites servers are located in various locations, including the UK and the US, and their group companies and third-party service providers and partners operate around the world. This means that when they collect personal information, they may process it in any of these countries. However, 8x8 states they have taken appropriate safeguards to require that personal information will remain protected in accordance with their Privacy Notice. These include implementing an intra-group agreement based on the European Commission's Standard Contractual Clauses for transfer of personal information between group companies. 8x8 Inc. also has certified to the European Union-United States Privacy Shield Framework and the United Stated-Swiss Privacy Shield Framework. 8x8 also requires such third parties to protect personal information they process from the European Economic Area ("EEA") in accordance with European Union data protection law. Further details can be provided upon request.

V. Clause about **Privacy Shield** [1]

VI. In their Privacy Notice 8x8 have a special section for EEA visitors only. For visitors from the European Economic Area, the legal basis for collecting and using personal

[1] 8x8 Inc. has certified certain services, for which they act as a data processor, under the EU-U.S. Privacy Shield framework. In the event of any conflict between the terms in this Privacy Notice and the Privacy Shield Principles, the Privacy Shield Principles shall govern.

Scope:

8x8 Inc. adheres to the principles of the EU-U.S. Privacy Shield framework with respect to personal data of individuals in the European Economic Area member states ("EU Individuals") included in the content of communications transmitted, received, or stored by 8x8 Inc.'s customers or by 8x8 Inc. on behalf of its customers in reliance on the Privacy Shield through the following services: 8x8 Virtual Office and 8x8 Virtual Contact Center ("Personal Data").

Data processed:

8x8 Inc. provides cloud communications services, including virtual private branch exchange and virtual contact center services, to business customers. In providing these services, 8x8 Inc. processes the communications customers transmit, receive, or store through 8x8 services or instruct 8x8 to process on their behalf. While 8x8 Inc.'s customers decide what, if any, Personal Data to include in such communications, it typically includes information about 8x8 Inc. customers' users, their current, prospective, or former customers, or any other person or entity communicating with 8x8 Inc. customers.

Purposes for which data is used:

information will depend on the personal information concerned and the specific context in which 8x8 collects it.

However, 8x8 will normally collect personal information only (i) where the processing is in their legitimate interests and not overridden by users' rights, (ii) where the processing is a contractual necessity, or (iii) where they have users' consent to do so. In some cases, they may also have a legal obligation to collect users' personal information or may otherwise need the personal information to protect users' vital interests or those of another person.

8x8 Inc. may use Personal Data for providing, managing, deploying, enhancing, or improving their services, as otherwise instructed by the 8x8 Inc. customer or other data controller who transmitted, received, or stored the data, or in accordance with contractual requirements. 8x8 Inc. may also use Personal Data for other purposes for which the customer or other data controller has obtained the relevant EU Individual's consent.

Inquiries and complaints:

An EU Individual covered by Privacy Shield and the Privacy Notice who believes that 8x8 Inc. maintains their Personal Data in one of the services within the scope of their Privacy Shield certification, such EU individual may submit any privacy or data use concerns concerning such data by email to privacypolicy@8x8.com or by mail to: **8x8, Inc.** 675 Creekside Way, Campbell, CA 95008, USA Attention: Privacy. 8x8 Inc. will respond within 45 days of receiving the communication. If user has an unresolved privacy or data use concern that 8x8 has not addressed satisfactorily, they should contact the U.S.-based third party dispute resolution provider (free of charge) at https://feedback-form.truste.com/watchdog/request.

If neither 8x8 Inc. nor the U.S.-based third party dispute resolution provider resolve the complaint, user may have the possibility to engage in binding arbitration as provided under the Privacy Shield Program (See Privacy Shield website).

Third parties who may receive Personal Data:

8x8 Inc. may disclose Personal Data to its affiliates, as well as to a limited number of third-party business partners, service providers, vendors, suppliers and other contractors (collectively, "Service Providers") for the purpose of assisting us in providing, managing, deploying, enhancing, or improving our services. 8x8 Inc. maintains contracts with these 8x8 Inc. affiliates and Service Providers restricting their access, use and disclosure of Personal Data in compliance with our Privacy Shield obligations, and 8x8 Inc. may be liable if such parties fail to meet those obligations and 8x8 are responsible for the event giving rise to the damage. 8x8 also may share or disclose Personal Data to the extent that the customer or other data controller has obtained the relevant EU Individual's consent.

User's rights to access, to limit use, and to limit disclosure:

EU Individuals have rights to access their stored Personal Data and to limit its use and disclosure. Under their Privacy Shield certification, 8x8 has committed to respect those rights. Because 8x8 Inc. personnel have limited ability to access data customers or other data controllers transmit, receive, or store through our services, EU Individuals covered by Privacy Shield and the Privacy Notice, who wish to request access to or to limit use or disclosure of their Personal Data, should provide the name of the 8x8 Inc. customer or other data controller who transmitted, received, or stored their Personal Data through 8x8 services. 8x8 will refer such request to that customer or other data controller and will support that business as needed in responding to user's request.

U.S. Federal Trade Commission enforcement:

8x8 Inc.'s commitments under the Privacy Shield are subject to the investigatory and enforcement powers of the United States Federal Trade Commission or the applicable United States authorized statutory body.

Compelled disclosure:

8x8 Inc. may be required to disclose Personal Data in response to lawful requests by public authorities, or administrative or judicial process, including to meet national security or law enforcement requirements.

If 8x8 asks the user to provide personal information to comply with a legal requirement or to enter into a contact with user's organization, they will make this clear at the relevant time and advise the user whether the provision of their personal information is mandatory or not (as well as of the possible consequences if user does not provide their personal information).
According to their statement, if they collect and use personal information in reliance on their legitimate interests (or those of any third party), this interest will normally be to operate their Websites or services and to communicate with users as necessary to provide their services to user's organization; as well as for their legitimate commercial interests, for instance, when responding to users' queries, improving their Website or services, undertaking marketing, or for the purposes of detecting or preventing illegal activities. They stipulate they may have other legitimate interests and if appropriate they will make clear to user at the relevant time what those legitimate interests are.
VII. The laws of the State of California, U.S.A., excluding California's conflict of laws rules, will apply to any disputes arising out of or relating to the Terms or the Service. All claims arising out of or relating to the Terms or the Service will be litigated exclusively in the federal or state courts of Santa Clara County, California, USA, and by accepting the use of the app the is also deemed to consent to personal jurisdiction in those courts.

4. TO WHAT EXTENT DO THE PLATFORM PROVIDERS SELL OR SHARE PERSONAL DATA?

According to the 8x8 Privacy Notice, they may disclose users' personal information to the following categories of recipients:

- to their **group companies, third party services providers and partners** who provide data processing services to them, for example (i) to support the delivery of, provide functionality on, or help to enhance the security of their Websites or services, (ii) for quality control and assurance, or (iii) improving their services and developing new services. They may also share personal information with such third parties where they consider that such disclosure is necessary to protect the safety or legitimate business interests of those third parties, including to investigate suspected fraud or to trace debtors.
- to any **competent law enforcement body, regulatory, government agency, court or other third party** where they believe disclosure is necessary (i) as a matter of applicable law or regulation, (ii) to exercise, establish or defend their legal rights, or (iii) to protect user's vital interests or those of any other person;
- to an **actual or potential buyer** (and its agents and advisers) in connection with any proposed purchase, merger or acquisition of any part of their business, provided that they inform the buyer it must use users' personal information only for the purposes disclosed in the Privacy Notice;
- to any **other person with users' consent** to the disclosure.

Furthermore, 8x8 Inc. may disclose Personal Data to its affiliates, as well as to a limited number of third-party business partners, service providers, vendors, suppliers and other contractors (collectively "Service Providers") for the purpose of assisting 8x8 in providing, managing, deploying, enhancing, or improving their services. 8x8 Inc. maintains

contracts with these 8x8 Inc. affiliates and Service Providers restricting their access, use and disclosure of Personal Data in compliance with Privacy Shield obligations, and 8x8 Inc. may be liable if such parties fail to meet those obligations and 8x8 are responsible for the event giving rise to the damage. 8x8 also may share or disclose Personal Data to the extent that the customer or other data controller has obtained the relevant EU Individual's consent.

5. To what surveillance might data held by the platform providers potentially be exposed?

8x8 Inc. may be required to disclose Personal Data in response to lawful requests by public authorities, or administrative or judicial process, including to meet national security or law enforcement requirements.
Security: 8x8 uses appropriate technical and organizational measures to protect the personal information that they collect and process about users. The measures they use are designed to provide a level of security appropriate to the risk of processing users' personal information. Specific measures they use include SSL encryption technology for protection of sensitive information such as payments when in transit. They have industry-standard administrative, technical and physical safeguards in place to protect the confidentiality, integrity and availability of personal information. Furthermore, in the US they are validated to HIPPAA and FISMA standards, and in the UK they are certified to ISO27001; ISO9000:2015 and Cyber Essentials certification schemes.

SECURITY CONCERNS FROM USERS
1.- According to the "Jitsi Meet Security & Privacy" in many respect Jitsi meetings are private by design. Meeting rooms are ephemeral and they are destroyed when the last participant leaves.
Nevertheless it was remarked that when you have created a link and close the chat, the room closes off, but, in the future if you re-enter the same room, anybody who had the original link can watch or listen to you without you knowing it.
2.- The official/security page states:
"Jitsi meetings can operate in 2 ways: peer-to-peer (P2P) or via the Jitsi Videobridge (JVB). This is transparent to the user. P2P mode is only used for 1-to-1 meetings. In this case, audio and video are encrypted using DTLS-SRTP all the way from the sender to the receiver, even if they traverse network components like TURN servers."
However, it seems that E2EE is only applicable in one-on-one communications whereas in cases of more than 2 participants in a room WebRTC currently does not provide the necessary tools to make E2EE possible.

- between 2 participants the call is E2E encrypted and p2p, so it seems very difficult if not impossible for "Big Bother" to listen/record
- between 3 participants the call is E2E encrypted, but not p2p, because the server needs to decrypt the video call, so if Big Brother has access to the server it can listen/record. In this case if YOU own the server the communication should still be secure

3.- Reports of unknown uninvited users/spies

4.- Reports of trolls invading a meeting room. In case the user is using their own server (instead of e.g. meet.jit.si) anybody having root in the server will be able to guess the room names and get possible access to the meeting room.
5.- Jitsi server trying to reach the internet, even when no meetings are happening. A firewall might stop the connection, but there are worries about this.
6.- Usually all users have the same powers, so anyone in the meeting room can change the password.
7. Recordings: The easiest way to record is to live stream the conference to YouTube and access the recording there. Self-installed Jitsi Meet deployments will need to setup Jibri to do this. The other way is to connect Dropbox with Jitsi meet and save the video in the Dropbox.

Kinly and StarLeaf

Kinly

Source: https://www.kinly.com/privacy/

Who is the data controller?

1. Kinly lists all entities that are controllers in the UK, Norway, USA and the Netherlands (but not Singapore). The Privacy Statement advises that the data controllers are country specific.
2. In the UK, the data controllers are:
    - Kinly Ltd
    - The Video Conference Bureau Ltd
    - Vision Connected United Kingdom Ltd
    - In the US, the data controller is:
    - Kinly Inc
3. In the Netherlands, the data controllers are:
    - Kinly Netherlands B.V.
    - MK2 Audiovisueel B.V.
    - MK2 Audiovisueel Verhuur B.V.
    - MK2 Group B.V.
4. In Norway, the data controllers are:
    - Kinly AS
    - VCV Nordics AS
    - Viju AS
5. The Security in the Kinly Cloud document, states that Kinly also has multiple Points of Presence (PoP) across the global. These are hosted at Data Centres managed by service providers, Google Cloud Platform, IBM Cloud and Baseform. Kinly states that the customer can choose which PoP they want to use (due to differing regulatory and policy requirements). The Points of Presence are located in:
    - Oslo, NO
    - London, UK
    - Frankfurt, DE
    - Singapore, MY
    - Ashburn, US
    - Finland, FI
    - Sao Paolo, BR

Where is the data stored?

1. Although the Privacy Statement is drafted in a straightforward way (making it easy to read), it is confusing when determining where Kinly actually stores its data.
2. The Privacy Statement advises that *"Hosting and storage of your data takes place in **data centers** located in the **United Kingdom, Netherlands, Norway and the USA.** We use 3rd party suppliers to store this information and have an agreement with them that protects your information."*

3. However, according to the document 'Security in the Kinly Cloud', all the data stored by the service is handled by Kinly Cloud-managed ISO27001-certified data centre in Oslo, Norway, or in Google Cloud data centres with encryption at rest for all data.
4. Further to this, the Security in the Kinly Cloud documents states that the PoP's are situated in Data Centers. Frankfurt, Singapore, Finland and Sao Paolo are not listed in the Privacy Statement as Data Centers and therefore, not all information can be stored in the Data Centers, like the Policy Statement suggests.
5. The Security in the Kinly Cloud document also states that only authorised personnel can access the data centre in Oslo, Norway. However, there is no definition of 'personnel'.

Length of storage

1. Kinly is vague when identifying how long it stores data for. The Privacy Notice states that *"Kinly does not store personal data longer than necessary for the purposes for which it is processed".*
2. It states that *"in general, we aim to retain customer/vendor personal data for no longer than two (2) years, unless a longer or shorter mandatory retention period applies or retention of the specific personal data is necessary."*
3. It states that it will not keep data for longer than the legislation/GDPR permits.

What types of data are stored?

1. The Security in the Kinly Cloud document states that it stores the following information on users/vendors and third-parties:
2. *Name, business e-mail address, business postal address, business telephone number, occupation/title, name of organization, department, industry, date of agreement, business facsimile number, VAT numbers, tax identification numbers, bank details.*
3. The Privacy Notice also states that it uses Hubspot as a processor to store personal data of people who request information from the site.

What are the most important aspects in the terms and conditions of the platform?

1. We could not find the terms and conditions for using Kinly in Europe.
2. The only accessible terms and conditions are the Terms and Conditions of Sale (US) for Kinly Inc (US Data Controller) – https://www.kinly.com/kinly-inc-terms-and-conditions-of-sale. This appears to be a pretty standard contract with no specific information mention of storing data or information.

To what extent do the platform providers sell or share personal data?

1. Within Kinly, personal data are only available to employees who must process them to achieve the stated objectives for data processing.
2. However, it also may share data with third parties either to fulfil a contract or to satisfy a legal obligation to which it is subject.
3. Kinly shares personal data with the following third parties: suppliers of IT-systems, processors, accountants, insurers, external legal counsel, regulators, affiliated companies, third-party service providers, advertising partners.

4. In its privacy policy, Kinly reiterates that any data sharing agreement will take place in full compliance with the GDPR.

To what surveillance might data held by the platform providers potentially be exposed?

6. As a company, Kinly is owned by Avedon Capital Partners based in the Netherlands.
7. However, Kinly's operations include international transfer of data between other group companies or this parties. As such, Kinly is located in United Kingdom, Norway, Netherlands and Singapore. Hosting and storage of data takes place in data centers located in the United Kingdom, Netherlands, Norway and the USA.
8. Therefore it is subject to laws of the countries where the data are stored.
9. Kinly uses third party suppliers to store this information and has relevant agreements to protect personal data.
10. For international data transfers within its companies, Kinly uses Standard Contractual Clauses.

- **StarLeaf**

Who is the data controller?

1. The controller is a party which enters into a Service Agreement with StarLeaf Ltd (which is a processor) registered in the UK. The terms are set out in the Data Processing Addendum: https://318jud367y2743qanus941sz-wpengine.netdna-ssl.com/wp-content/uploads/guides/starleaf_dpa_v5.4.pdf .
2. If a StarLeaf subscription was purchased through a partner or reseller, StarLeaf received that information via that agency. The reseller and partner works with StarLeaf to ensure that the service can be activated, and they serve as a Data Controller ("Controller") whereas StarLeaf is acting as a Data Processor ("Processor").
3. StarLeaf also states that it '*may also collect information about your service usage that is generated by your StarLeaf subscription. This data is helpful for service operations activities such as troubleshooting, diagnostics and capacity trending*.'
4. The privacy policy includes the details of the Data Protection Officer (**DPO**) who is registered with the UK Information Commissioners Office (**ICO**).

Where is the data stored?

1. The data is stored in a variety of locations depending on where the user is located. StarLeaf has multiple geographically dispersed Points of Presence (**PoP**) and it is possible for the users to be moved between them '*as required to protect against any catastrophic local events that prevent access to a whole data center*.' More: https://www.starleaf.com/assets/Uploads/starleaf-security-white-paper-2018-1.pdf
2. In its legal notice (https://support.starleaf.com/legal-information/starleaf-and-gdpr-compliance/), StarLeaf states that '*While account profile data is kept for the duration of the active account, call records are anonymised after 90 days, meaning the details of the calls and associated diagnostics are deleted at that threshold. We do this to comply with the requirement not to keep data "longer than is necessary*.'

What are the most important aspects in the terms and conditions of the platform?

1. Several legal mechanisms are employed to facilitate international data transfers. When using other processors located in the United States, StarLeaf ensures it is certified under the EU-U.S. Privacy Shield Framework, providing a level of protection in line with EU data protection law. This includes processors such as Google, MailChimp, Freshdesk, Salesforce, Plivo, Twilio, Sendgrid and AWS.
2. StarLeaf also monitors other developing regulations that will require non-EU international transfer mechanisms, and states it is committed to maintaining lawful compliance with all such applicable laws.
3. StarLeaf acknowledges third party software that is used in its products: https://support.starleaf.com/legal-information/third-party-acknowledgements/.

To what extent do the platform providers sell or share personal data?

1. StarLeaf assures that it does not use or share personal information in any other way beyond what has been written in their privacy policy. They also assure they do not sell personal information to anyone, including but not limited to third parties for their own marketing use.
2. '*As a data processor, StarLeaf is acting under the instructions of the data controller, and may share your data with the controller in support of your service. The controller has administrative access to the StarLeaf portal, and may access call detail records for the purpose of troubleshooting, diagnostics, capacity management, billing and reporting. It should be noted that the content of your video meetings is not shared with anyone, and this capability does not exist in the administrative portal.*'
3. Importantly, StarLeaf states that in cases where service subscription includes conference recording capability, it integrates with its partner Media Network Services AS (MNS) in Oslo, Norway to provide that service. A copy of the MNS privacy policy is available to read here: https://www.mns.vc/privacy/.
4. The MNS privacy notices states that the MNS can appear both as a controller (in cases where services were purchased directly with them) and a processor (if the service was bought through a service provider or reseller).
5. StarLeaf may also share data with its subprocessors who facilitate the delivery of its service, which could include G-Suite, MailChimp, Freshdesk, Salesforce, Pardot, Plivo, Twilio, and Sendgrid. StarLeaf states that '*For each entity, a data processing agreement exists between StarLeaf and the subprocessor, with matching flow-down terms outlining sufficient guarantees of technical safeguards for the protection of personal information.*'

To what surveillance might data held by the platform providers potentially be exposed?

1. StarLeaf may be subject to surveillance laws of several countries depending where the data is located.
2. StarLeaf asserts that the content of the calls cannot be accessed by its employees or any third party: https://support.starleaf.com/legal-information/starleaf-privacy-notice/. Also '*Calls are not monitored or recorded, except for videomail and voicemail messages, and calls which are explicitly recorded and saved by our customers using StarLeaf's recording services products*.' These cannot be accessed by anyone outside of StarLeaf.
3. Importantly, StarLeaf mentions in their notice that it will: '*inform you or your data controller if we are required to share your information under any of the following circumstances: (i) to the extent that we are required to do so by applicable law, by a governmental body or by a law enforcement agency, or for crime prevention*

purposes; (ii) in connection with any legal proceedings (including prospective legal proceedings); (iii) in order to establish or defend our legal rights; (iv) in the event that we buy or sell any business or assets, in which case we may disclose your personal data to the prospective sellers or buyer of such business or assets; or (v) if a third party acquires all (or substantially all) of our business and/or assets, we may disclose your personal information to that third party in connection with the acquisition.'

Messenger Video

For the Messenger video service, the user is referred to the Data Policy dated April 2018 which is common for Facebook, Instagram, Messenger and other products and features offered by Facebook.

1. WHO IS THE DATA CONTROLLER

The data controller is Facebook Ireland Ltd, 4 Grand Canal Square, Grand Canal Harbour, Dublin 2 Ireland

2. WHERE IS THE DATA STORED

Information controlled by Facebook Ireland will be transferred or transmitted to, or stored and processed in, the United States or other countries for the purposes described in the Data Policy.

Data is stored until it is no longer necessary to provide services and Facebook Products or until user account is deleted – whichever comes first. This is a case-by-case determination that depends on things such as the nature of the data, why it is collected and processed, and relevant legal or operational retention needs. For example, when the user searches for something on Facebook, they can access and delete that query from within users' search history at any time, but the log of that search is deleted after six months. If user submits a copy of a valid photo ID for account verification purposes, Facebook deletes that copy 30 days after submission.

When the account is deleted, Facebook deletes things that user has posted, such as photos and status updates, and users won't be able to recover this information later. Information that others have shared about the user isn't part of user's account and won't be deleted. If users don't want to delete their account but want to temporarily stop using the Products, they can deactivate your account instead.

3. WHAT ARE THE MOST IMPORTANT ASPECTS IN THE TERMS AND CONDITIONS OF THE PLATFORM?

I. In the Data Policy there is extensive reference to the information and data collected by the Facebook Products and how this information is used, i.e. information & content provided by the user, networks and connections, usage, transactions, device information etc.

II. Face recognition: If turned on by the user, FB uses face recognition technology to recognize the user in photos, videos and camera experiences. The face-recognition templates FB creates are data with special protections under EU law.

III. Facebook and Instagram share infrastructure, systems and technology with other Facebook Companies (which include WhatsApp and Oculus) with the aim to provide an innovative, relevant, consistent and safe experience across all Facebook Company Products. They also process information about users across the Facebook Companies for these purposes, as permitted by applicable law and in accordance with their terms and policies. For example, they process information from WhatsApp about accounts sending spam on its service so they can take appropriate action against those accounts on Facebook, Instagram or Messenger. They also work to understand how people use and interact with Facebook Company Products, such as understanding the number of unique users on different Facebook Company Products.

IV. As per the FB Terms and Conditions, for consumers habitually residing in a Member State of the European Union, the laws of that Member State will apply to any claim, cause of action or dispute against FB, which arises out of or relates to the Terms or the Facebook Products, and users may resolve their claims in any competent court in that Member State that has jurisdiction over the claim. In all other cases, user agrees that the claim must be resolved in a competent court in the Republic of Ireland and that Irish law will govern any claim, without regard to conflict of law provisions.

4. TO WHAT EXTENT DO THE PLATFORM PROVIDERS SELL OR SHARE PERSONAL DATA?

FB utilizes standard contractual clauses approved by the European Commission and rely on the European Commission's adequacy decisions about certain countries, as applicable, for data transfers from the EEA to the United States and other countries.

Facebook warns about visibility of personal data shared by the user or other people in the user's social network.

Devices and operating systems providing native versions of Facebook and Instagram (i.e. where FB/Insta have not developed their own first-party apps) will have access to all information users choose to share with them, including information users' friends share with them, so they can provide FB/Insta core functionality to users.

Allegedly FB is in the process of restricting developers' data access even further to help prevent abuse. For example, FB will remove developers' access to user's Facebook and Instagram data if user hasn't used their app in 3 months, and FB are changing Login, so that in the next version, FB will reduce the data that an app can request without app review to include only name, Instagram username and bio, profile photo and email address. Requesting any other data will require FB approval.

Other than public information and content shared/reshared by users FB Data Policy stipulates the following cases for transferring information to third parties:

I. New owner. If the ownership or control of all or part of FB Products or their assets changes, FB may transfer personal information to the new owner.

II. Sharing with Third-Party Partners. FB works with third-party partners who help provide and improve FB Products or who use Facebook Business Tools to grow their businesses. FB doesn't sell any of users' information to anyone, and they claim they never will. FB also imposes strict restrictions on how their partners can use and disclose the data FB provides. The types of third parties FB share information with are as follows:

> (a) Partners who use FB analytics services. FB provides aggregated statistics and insights that help people and businesses understand how people are engaging with their posts, listings, Pages, videos and other content on and off the Facebook Products. For example, Page admins and Instagram business profiles receive information about the number of people or accounts who viewed, reacted to, or commented on their posts, as well as aggregate demographic and other information that helps them understand interactions with their Page or account.
>
> (b) Advertisers. FB provide advertisers with reports about the kinds of people seeing their ads and how their ads are performing, but FB doesn't share information that personally identifies the user (information such as name or email

address that by itself can be used to contact the user or identifies who the user is) unless the user gives permission. For example, FB provides general demographic and interest information to advertisers (for example, that an ad was seen by a woman between the ages of 25 and 34 who lives in Madrid and likes software engineering) to help them better understand their audience. FB also confirms which Facebook ads led the user to make a purchase or take an action with an advertiser.

(c) Measurement partners. FB shares information about users with companies that aggregate it to provide analytics and measurement reports to FB partners.

(d) Partners offering goods and services in FB Products. When the user subscribes to receive premium content, or buy something from a seller in FB Products, the content creator or seller can receive user's public information and other information the user shares with them, as well as the information needed to complete the transaction, including shipping and contact details.

(e) Vendors and service providers. FB provides information and content to vendors and service providers who support FB business, such as by providing technical infrastructure services, analyzing how FB Products are used, providing customer service, facilitating payments or conducting surveys.

(f) Researchers and academics. FB also provides information and content to research partners and academics to conduct research that advances scholarship and innovation that support the business or mission of FB, and enhances discovery and innovation on topics of general social welfare, technological advancement, public interest, health and well-being.

(g) Law enforcement or legal requests. FB accesses, preserves and shares users' information with regulators, law enforcement or others: (i) In response to a legal request, if FB has a good-faith belief that the law requires them to do so. FB can also respond to legal requests when they have a good-faith belief that the response is required by law in that jurisdiction, affects users in that jurisdiction, and is consistent with internationally recognized standards. (ii) When FB has a good-faith belief it is necessary to: detect, prevent and address fraud, unauthorized use of the Products, violations of FB terms or policies, or other harmful or illegal activity; to protect FB (including their rights, property or Products), the user or others, including as part of investigations or regulatory inquiries; or to prevent death or imminent bodily harm. For example, if relevant, FB provides information to and receives information from third-party partners about the reliability of the user's account to prevent fraud, abuse and other harmful activity on and off FB Products.

(h) Information FB receives about users (including financial transaction data related to purchases made with Facebook) can be accessed and preserved for an extended period when it is the subject of a legal request or obligation, governmental investigation, or investigations of possible violations of our terms or policies, or otherwise to prevent harm. They also retain information from accounts disabled for terms violations for at least a year to prevent repeat abuse or other term violations.

5. TO WHAT SURVEILLANCE MIGHT DATA HELD BY THE PLATFORM PROVIDERS POTENTIALLY BE EXPOSED?

See 4.II (g) and (h) above

Skype, Skype for Business and Poly.com

- **Skype and Skype for Business**

Software operated by Microsoft. Skype is intended for consumer use wherease Skype for Business, as the name reveals, aims at professional use.

For both, the basic privacy document is the Microsoft Privacy Statement. In includes general terms of Microsoft's approach to data use and product specific details, including Skype. The Enterprise and developer products section of the privacy statement applies to Skype for Business use (also see below).

Microsoft Services Agreement then applies to the terms of use of Microsoft products, including Skype specific terms.

It should be noted that *"Microsoft® Teams replaces Skype for Business Online as Microsoft's professional online meeting solution."*[2] For Teams, reference is made to the above analysis.

1. Who is the data controller?

For those in the European Economic Area, the United Kingdom, and Switzerland (see contact us section of the Privacy statement):

Microsoft Ireland Operations Limited
One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, Ireland. Telephone: +353 1 706 3117.

2. Where is the data stored?

Privacy statement:
Personal data collected by Microsoft may be stored and processed in your region, in the United States, and in any other country where Microsoft or its affiliates, subsidiaries, or service providers operate facilities. Microsoft maintains major data centres in Australia, Austria, Brazil, Canada, Chile, Finland, France, Germany, Hong Kong, India, Ireland, Japan, Korea, Luxembourg, Malaysia, the Netherlands, Singapore, South Africa, the United Kingdom and the United States. Typically, the primary storage location is in the customer's region or in the United States, often with a backup to a data centre in another region. The storage location(s) are chosen in order to operate efficiently, to improve performance, and to create redundancies in order to protect the data in the event of an outage or other problem. We take steps to ensure that the data we collect under this privacy statement is processed according to the provisions of this statement and the requirements of applicable law wherever the data is located.

We transfer personal data from the European Economic Area, the United Kingdom, and Switzerland to other countries, some of which have not yet

[2] Cited from https://www.skype.com/en/business/

been determined by the European Commission to have an adequate level of data protection. For example, their laws may not guarantee you the same rights, or there may not be a privacy supervisory authority there that is capable of addressing your complaints. When we engage in such transfers, we use a variety of legal mechanisms, including contracts, to help ensure your rights and protections travel with your data. To learn more about the European Commission's decisions on the adequacy of the protection of personal data in the countries where Microsoft processes personal data, see this article on the European Commission website.

Microsoft Corporation complies with the EU-U.S. Privacy Shield Framework and Swiss-U.S. Privacy Shield Framework as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal information transferred from the European Union, the United Kingdom, and Switzerland to the United States. Microsoft Corporation has certified to the Department of Commerce that it adheres to the Privacy Shield Principles. If third-party agents process personal data on our behalf in a manner inconsistent with the principles of either Privacy Shield framework, we remain liable unless we prove we are not responsible for the event giving rise to the damage. The controlled U.S. subsidiaries of Microsoft Corporation, as identified in our self-certification submission, also adhere to the Privacy Shield Principles—for more info, see the list of Microsoft U.S. entities or subsidiaries adhering to the Privacy Shield Principles.

If there is any conflict between the terms in this privacy policy and the Privacy Shield Principles, the Privacy Shield Principles shall govern. To learn more about the Privacy Shield programme, and to view our certification, visit the Privacy Shield website.

If you have a question or complaint related to participation by Microsoft in the EU-U.S. or Swiss-U.S. Privacy Shield, we encourage you to contact us via our web form. For any complaints related to the Privacy Shield frameworks that Microsoft cannot resolve directly, we have chosen to cooperate with the relevant EU Data Protection Authority, or a panel established by the European data protection authorities, for resolving disputes with EU individuals, and with the Swiss Federal Data Protection and Information Commissioner (FDPIC) for resolving disputes with Swiss individuals. Please contact us if you'd like us to direct you to your data protection authority contacts. As further explained in the Privacy Shield Principles, binding arbitration is available to address residual complaints not resolved by other means. Microsoft is subject to the investigatory and enforcement powers of the U.S. Federal Trade Commission (FTC).

3. What are the most important aspects in the terms and conditions of the platform?

Data may be stored in U.S. and accessed by LEA

For data collected by Skype and Skype for Business see below (Section on product specific details of the Privacy statement).

4. To what extent do the platform providers sell or share personal data?

Privacy statement: Section “Reasons we share personal data”:

> We share your personal data with your consent or as necessary to complete any transaction or provide any product you have requested or authorised. For example, we share your content with third parties when you tell us to do so, such as when you send an email to a friend, share photos and documents on OneDrive, or link accounts with another service. If you use a Microsoft product provided by an organisation you are affiliated with, such as an employer or school, or use an email address provided by such organisation to access Microsoft products, we share certain data, such as interaction data and diagnostic data, to enable your organisation to manage the products. When you provide payment data to make a purchase, we will share payment data with banks and other entities that process payment transactions or provide other financial services, and for fraud prevention and credit risk reduction.
>
> In addition, we share personal data among Microsoft-controlled affiliates and subsidiaries. We also share personal data with vendors or agents working on our behalf for the purposes described in this statement. For example, companies we've hired to provide customer service support or assist in protecting and securing our systems and services may need access to personal data to provide those functions. In such cases, these companies must abide by our data privacy and security requirements and are not allowed to use personal data they receive from us for any other purpose. We may also disclose personal data as part of a corporate transaction such as a merger or sale of assets.
>
> Finally, we will retain, access, transfer, disclose, and preserve personal data, including your content (such as the content of your emails in Outlook.com, or files in private folders on OneDrive), when we have a good faith belief that doing so is necessary to do any of the following:
>
> - Comply with applicable law or respond to valid legal process, including from law enforcement or other government agencies.
> - Protect our customers, for example, to prevent spam or attempts to defraud users of our products, or to help prevent the loss of life or serious injury of anyone.
> - Operate and maintain the security of our products, including to prevent or stop an attack on our computer systems or networks.
> - Protect the rights or property of Microsoft, including enforcing the terms governing the use of the services—however, if we receive information indicating that someone is using our services to traffic in stolen intellectual or physical property of Microsoft, we will not inspect a customer's private content ourselves, but we may refer the matter to law enforcement.

For more information about data we disclose in response to requests from law enforcement and other government agencies, please see our Law Enforcement Requests Report.

Please note that some of our products include links to or otherwise enable you to access products of third parties whose privacy practices differ from those of Microsoft. If you provide personal data to any of those products, your data is governed by their privacy policies.

5. To what surveillance might data held by the platform providers potentially be exposed?

See answer to question no. 4

Also, see FAQs to the Law Enforcement Requests Report – includes detailed overview of Microsoft's approach to government requests for data.

Privacy statement – Product specific details – Skype:

Skype lets you send and receive voice, video, SMS, and instant message communications. This section applies to the consumer version of Skype; if you are using Skype for Business, see the Enterprise and developer products section of this privacy statement.

As part of providing these features, Microsoft collects usage data about your communications that includes the time and date of the communication and the numbers or user names that are part of the communication.

Skype profile. Your Skype profile includes information you provided when you set up a Microsoft account. To enable other people to find you on Skype (or products that interact with Skype, such as Skype for Business), depending on your profile settings, your Skype profile is included in the Skype public search directory and may be recommended to other users. Your profile includes your user name, avatar, and any other data you choose to add to your profile or display to others.

Skype Contacts. If you use a Microsoft service, such as Outlook.com, to manage contacts, Skype will automatically add the people you know to your Skype contact list until you tell us to stop. With your permission, Skype will also check your device or other address books to automatically add your friends as Skype contacts. You can block users if you don't want to receive their communications.

Partner companies. To make Skype available to more people, we partner with other companies to allow Skype to be offered via those companies' services. If you use Skype through a company other than Microsoft, that company's privacy policy governs how it handles your data. To comply with applicable law or respond to valid legal process, or to help our partner company or local operator comply or respond, we may access, transfer, disclose, and preserve your data. That data could include, for example, your private content, such as the content of your instant messages, stored video messages, voicemails, or file transfers.

Skype Manager. Skype Manager lets you manage a group's (such as your family's) Skype usage from one central place. When you set up a group, you will be the Skype Manager Administrator and can see the patterns of usage, including detailed information, like traffic data and details of purchases, of other members of the group who have consented to such access. If you add information like your name, other people in the group will be able to see it. Members of the group can withdraw consent for Skype Manager by visiting their Skype account page.

Push notifications. To let you know of incoming calls, chats, and other messages, Skype apps use the notification service on your device. For many devices, these services are

provided by another company. To tell you who is calling, for example, or to give you the first few words of the new chat, Skype has to tell the notification service so that they can provide the notification to you. The company providing the notification service on your device will use this information in accordance with their own terms and privacy policy. Microsoft is not responsible for the data collected by the company providing the notification service. If you don't want to use the notification services for incoming Skype calls and messages, turn it off in the settings found in the Skype application or your device.

Translation features. To help you communicate with people in different languages, some Skype apps offer audio and/or text translation features. When you use translation features, your voice and text data are used to provide and improve Microsoft speech recognition and translation services.

Recording features. Some versions of Skype have a recording feature that allows you to capture and share all or part of your audio / video call. The recording will be stored and shared as part of your conversation history with the person or group with whom the call occurred. You should understand your legal responsibilities before recording any communication. This includes whether you need to get consent from all parties to the communication in advance. Microsoft is not responsible for how you use your recordings or the recording features.

Skype bots. Bots are programs offered by Microsoft or third parties that can do many useful things like search for news, play games, and more. Depending on their capabilities, bots may have access to your display name, Skype ID, country, region, language, and any messages, audio, video, or content that you share with the bot. Please review the bot profile and its privacy statement before engaging in a one-to-one or group conversation with a bot. You can delete a bot that you no longer wish to engage with. Prior to adding a bot to a group, please ensure that your group participants have consented to their information being shared with the bot.

Recommendations in Skype. Subject to availability, Skype may offer suggestions to help you manage your time, tasks, find information and get things done. For example, Skype may provide contextual prompts to create reminders or suggest you create a task using Microsoft services.This data may also be used to improve Microsoft products.

Captioning. Certain Skype features include accessibility functionality such as captioning. During Skype calls, a call participant can activate a voice-to-text feature, which allows the user to view the audio chat as text. If a user activates this feature, other call participants will not receive a notification. Microsoft uses this voice and text data to provide captioning of audio for users.

Privacy statement – Product specific details - Enterprise online services (relevant for Skype for Business)

To provide the Enterprise Online Services, Microsoft uses data you provide (including Customer Data, Personal Data, Administrator Data, Payment Data, and Support Data) and data Microsoft collects or generates associated with your use of the Enterprise Online Services. We process data as described in the Online Services Terms (OST) and the Microsoft Trust Center.

Personal Data. Customer is the controller of Personal Data and Microsoft is the processor of such data, except when (a) Customer acts as a processor of Personal Data, in which case Microsoft is a subprocessor, (b) Microsoft is processing Personal Data for its legitimate business operations, in which case Microsoft is a controller, or (c) stated otherwise in the OST. Microsoft is a controller of Personal Data when processing Personal Data for its legitimate business operations associated with providing the service, such as billing and preparing invoices; account management; compensation; financial reporting; business planning and product strategy; improving core functionality for accessibility, privacy, and energy efficiency; and combatting fraud, cybercrime, and cyberattacks on Microsoft products. We generally aggregate Personal Data before using it for our legitimate business operations, removing the ability to identify specific individuals. We use personal data in the least identifiable form that will support processing necessary for legitimate business operations.

Administrator Data. Administrator Data is the information provided to Microsoft during sign-up, purchase, or administration of Enterprise Online Services. We use Administrator Data to provide the Enterprise Online Services, complete transactions, service the account, detect and prevent fraud, and comply with our legal obligations. Administrator Data includes the name, address, phone number, and email address you provide, as well as aggregated usage data related to your account, such as the controls you select. Administrator Data also includes contact information of your colleagues and friends if you agree to provide it to Microsoft for the limited purpose of sending them an invitation to use the Enterprise Online Services; we contact those individuals with communications that include information about you, such as your name and profile photo.

As needed, we use Administrator Data to contact you to provide information about your account, subscriptions, billing, and updates to the Enterprise Online Services, including information about new features, security, or other technical issues. We also contact you regarding third-party inquiries we receive regarding use of the Enterprise Online Services, as described in your agreement. You cannot unsubscribe from these non-promotional communications. We may also contact you regarding information and offers about other products and services, or share your contact information with Microsoft's partners. When such a partner has specific services or solutions to meet your needs, or to optimize your use of the Enterprise Online Services, we may share limited, aggregated information about your organization’s account with the partner. Microsoft will not share your confidential information or contact information with the authorized partner unless we have sufficient rights to do so. You can manage your contact preferences or update your information in your account profile.

Payment Data. We use payment data to complete transactions, as well as to detect and prevent fraud.

Support Data. Customers provide or authorize Microsoft to collect data in connection with obtaining technical support for the Enterprise Online Services. We process Support Data to provide technical support and as described in the OST.

Some Enterprise Online Services require, or are enhanced by, the installation of local software (e.g., agents, device management applications) on a device. At your direction, the local software may transmit (i) data, which can include Customer Data, from a device or appliance to or from the Enterprise Online Services; or (ii) logs or error reports to Microsoft for troubleshooting purposes. The Enterprise Online Services, including local software, collect device and usage data that is transmitted to Microsoft and analyzed to improve the quality, security, and integrity of our products.

Bing Search Services, as defined in the OST, use data such as search queries as described in the Bing section of this privacy statement.

- **Poly.com**

Poly is a hardware and service provider of telephone and videoconferencing tools. For example, the Czech Courts, Prosecutors and Prison Service uses Poly.com for their videoconferencing needs, including court hearings.

For Privacy issues the general privacy policy and product specific white papers apply.

1. Who is the data controller?

Plantronics, Inc.,
345 Encinal Street
Santa Cruz, California 95060 USA

Information on Poly's subprocessors can be found here.

2. Where is the data stored?

You agree that all Personal Information collected by Poly may be transferred, Processed, and stored anywhere in the world, including but not limited to, the United States, Australia, Singapore, or Ireland, as well as the European Union, in the cloud, on our servers, on the servers of our affiliates or the servers of our Service Providers, our group companies, and partners that may operate around the world

3. What are the most important aspects in the terms and conditions of the platform?

With regards to the Polycom RealPresence DMA platform, which is the platform the Czech judicial authorities use, see the security and privacy white paper. Page 4-6 refers to Data processing, its purpose, data storage and protection.

To summarize, RealPresence DMA does not access any customer's data except as required to enable the features provided by the application. As these systems are deployed in the customer's environment, it is the responsibility of the customer to protect data privacy.

RealPresence DMA collects and processes logs containing the following information: Device data, Call and conference data.

Poly collects data to understand how customers use the RealPresence DMA system. The system sends usage data once per hour over a secured (TLS) connection (port 8443) to a Poly collection point. The administrator can disable or enable data collection. All data is anonymized before sending and is thus scrubbed of any identifying information.

Poly does not upload any personal data. Analytics excludes all information that identifies individual people or an individual's habits.

The analytics data is stored in Amazon Web Services (AWS). Currently, we use data centers in the United States only. For transferring personal data of EU customers to the US, Poly uses an Intragroup Data Transfer Agreement incorporating the EU Standard Contractual Clauses as the transfer mechanism. Only approved Poly staff are allowed direct access to the data.

4. To what extent do the platform providers sell or share personal data?

Based on the general privacy policy, Poly:

We may share your information as described in this Privacy Policy; e.g., with a Third-Party or Service Providers, to comply with legal obligations, to protect and defend our rights and property, or with your permission.

Service Providers. From time to time, we may disclose your Personal Information to organizations that perform Services. For example, to provide customer Service, deliver Products, ship items, Process credit cards, for research, marketing, Product ratings and reviews, data Processing, and to measure the use of our Sites. We will only share the Personal Information necessary for these companies to perform work on our behalf. Your Personal Information will be provided to these organizations pursuant to a written agreement that prevents them from retaining, using, or disclosing the Personal Information for any reason other than the purpose of providing Services under the instructions of Poly, and with respect to that information, to keep it secure and act in a manner consistent with the relevant principles articulated in this Privacy Policy.

Compliance with Law. We may disclose your data to any competent law enforcement body, regulatory, government agency, court or other Third-Party where we believe disclosure is necessary, for example, (i) as a matter of applicable law or regulation, (ii) to exercise, establish or defend our legal rights, or (iii) to protect your vital interests or those of any other person.

Poly Partners. If you have opted-in to receive direct marketing contact from a Poly Partner, Poly will disclose your Personal information to the Poly Partners. Your Personal Information will be provided to the Poly Partner only if they agree to act in a manner consistent with the relevant principles articulated in this Privacy Policy. However, Poly recommends that you review the partner's privacy policy as their privacy practices are not monitored or controlled by Poly.

Mergers and Acquisitions. We may disclose your data to a potential buyer (and its agents and advisors) in connection with any proposed purchase, merger or acquisition of any part of our business, provided we inform the buyer it must use your Personal Information only for the purposes disclosed in this Privacy Policy. If Poly is involved in a merger, acquisition, or sale of all or a portion of its assets, you will be notified via email and/or a prominent notice on our Sites of any change in ownership.

5. To what surveillance might data held by the platform providers potentially be exposed?

See answer to question no. 4