

noyb

Report on privacy policies of video conferencing services



Table of Contents

1.	Introduction.....	3
2.	The review of video conferencing tools.....	3
2.1	Evaluation measures.....	4
2.1.1	Elements under Article 13 GDPR (“Privacy Policy”)	4
2.1.2	Measurement criteria.....	7
2.3	General observations: Poor structures and frequent changes.....	9
2.3.1	Controllershship versus processorship	9
2.3.2	Privacy policies are too generic.....	10
2.3.3	Missing link between categories of data, purposes of processing, and the legal basis for each purpose	10
2.3.4	In case of legitimate interests: the interests of the controller or third parties.....	11
2.3.5	Non-transparent data sharing / disclosure.....	11
2.3.6	Inadequate information about data being transferred abroad	12
2.3.7	Unclear information about how long data is stored.....	12
2.3.8	Misleading information about GDPR rights	12
2.3.9	Name and contact details were mostly provided	13
3.	Conclusion	13

1. Introduction

The outbreak of the SARS-CoV-2 pandemic has forced many people to work from home. This has been made possible through video conferencing tools and other remote means of communication, which have transformed our homes into our offices. They also help keep us connected with friends and family, regardless of where they are.

The adoption of video conferencing tools over the last weeks has been impressive. Microsoft's video and audio chat service, Skype, has witnessed a 70% increase of daily users compared to one month ago, with 40 million people using it on a daily basis.¹ The other tools, Cisco's Webex Meetings and Zoom, have also reported record usage of their services over the last two months.²

Video conferencing tools literally open a lens into our homes. The personal and professional spheres are increasingly merging. We phone with our parents and children, discuss business strategy with our colleagues, and perhaps relax with our yoga teacher after work, following her flow in front of our screen.

While we appreciate how video conferencing tool providers facilitate all this, the intimacy they permit calls for an equally intimate look into their compliance with EU data protection law.

2. The review of video conferencing tools

Against this backdrop, *noyb* evaluated the compliance of larger actors in the web conferencing industry with certain principles of the General Data Protection Regulation ("GDPR"). The services investigated were: Zoom, Webex Meetings (Cisco), Meeting (LogMeIn), Skype and Teams (both Microsoft), and Wire.

The GDPR obliges companies to provide information about the use of personal data and to inform users ("data subjects" in the terminology of the GDPR) about their data protection rights (Articles 13 and 14 GDPR). Article 12(1) GDPR further requires that all such information must be concise, transparent, and easily accessible, using clear and plain language. This is to ensure that privacy policies are understandable to the average person and not just to lawyers.

The investigation focused on this duty to provide proper information. Companies usually do so in a so-called "privacy policy", which *noyb* assessed.

It is important to note that we did not assess the services from a technical perspective. Some services, such as Zoom and Wire, claim to use end-to-end encryption. This type of encryption would render all communication content only visible to the actual participants and not to the service providers - something very much appreciated from a privacy perspective.

However, Zoom's claims have been shown to be misleading and false. Zoom does not actually use end-to-end encryption as commonly understood, but only transport layer encryption that leaves the

¹ Ian Sherr, "Microsoft's Skype sees massive increase in usage as coronavirus spreads" (cnet, 30 March 2020), accessed 31.03.2020, available at <https://www.cnet.com/news/microsofts-skype-sees-massive-increase-in-usage-as-coronavirus-spreads/>

² Jordan Novet, "Cisco says Webex video-calling service is seeing record usage too, even as competitor Zoom draws all the attention" (CNBC, 17 March 2020), accessed 31.03.2020, available at: <https://www.cnbc.com/2020/03/17/cisco-webex-sees-record-usage-during-coronavirus-expansion-like-zoom.html>

communication content visible to Zoom.³ Similarly, Zoom appears to also have poorly implemented their “Company Directory” feature, leaking both email addresses and photos.⁴

Independent technical verification of security and privacy is essential - both on a technical and organisational level.

2.1 Evaluation measures

2.1.1 Elements under Article 13 GDPR (“Privacy Policy”)

Processing of personal data should be lawful, fair, and transparent. The GDPR enshrines these principles in Article 5(1)(a) and the recitals. In particular, Recital 60 GDPR explains that a data controller should provide a data subject with all information necessary to ensure fair and transparent processing, taking into account the specific circumstances. Moreover, “*the data subject should be able to determine in advance what the scope and consequences of the processing entails*”.⁵

Articles 12–14 GDPR specify in more detail how and which information should be provided. Usually this is done in a so-called “privacy policy”. We restricted our investigation to Articles 12 and 13 GDPR. This means we focused on the information requirements where personal data is collected from the data subject (Article 13 GDPR). This is in contrast to where personal data is obtained from another source. In such a case, Article 14 GDPR states which information shall be provided. However, most elements in Article 14 GDPR overlap with the elements in Article 13 GDPR. We did not assess the extra elements of Article 14 GDPR.

The following section explains how we evaluated the individual elements under Article 13 GDPR.

- **Identity and contact details of the controller**

The name and contact details of the controller (i.e. the company processing the personal data) should be provided, ideally including “*different forms of communications with the data controller (e.g. phone number, email, postal address, etc.)*”.⁶ Looked at in light of the fairness principle enshrined in Article 5(1)(a) GDPR, but also interpreted against Article 5(1)(c) of the E-Commerce-Directive (2000/31/EC), we expected that electronic contact details were given because the investigated services are digital in nature. Only providing a postal address would be insufficient, as unfair in the context of such a service. We also believe that a mere online contact form is insufficient. For one, a form is a contact method and not a contact detail. For another, it artificially prevents the user from contacting the controller through the method of their choice - which is against Article 12(2) GDPR that requires a controller to facilitate the exercise of data subject rights.

³ Micah Lee, Yael Grauer “Zoom meetings aren’t end-to-end encrypted, despite misleading marketing” (The Intercept, 31 March 2020), accessed 1.4.2020, available at <https://theintercept.com/2020/03/31/zoom-meeting-encryption/>

⁴ Joseph Cox “Zoom is leaking peoples’ email addresses and photos to strangers” (Motherboard, Tech by Vice, 1 April 2020), accessed 2.4.2020, available at https://www.vice.com/en_us/article/k7e95m/zoom-leaking-email-addresses-photos

⁵ Article 29 Working Party “Guidelines on transparency under Regulation 2016/679”, WP260 rev.01, p. 7.

⁶ Article 29 Working Party “Guidelines on transparency under Regulation 2016/679”, WP260 rev.01, p. 35.

- **Contact details of the Data Protection Officer (DPO)**

The contact details of the Data Protection Officer (DPO) should be provided, where applicable (not all controllers are required to appoint a DPO). Providing the DPO's contact details should make it easy for data subjects and the supervisory authorities to reach the DPO, e.g. via a postal address, a dedicated telephone number, and/or a dedicated e-mail address.⁷ Looked at in light of the GDPR's fairness principle, we expected electronic contact details because the investigated services are digital in nature. Only providing a postal address would be insufficient, as unfair in the context of a streaming service. We also believe that a mere online contact form is insufficient. For one, a form is a contact method and not a contact detail. For another, it artificially prevents the user from contacting the controller through the method of their choice.

It must be noted that the GDPR does not require a controller to disclose the name of the Data Protection Officer. Contact details as just described are considered sufficient.

- **Purposes of processing; legal bases for processing; link between categories of personal data, purposes, and legal bases**

The controller should provide the purposes for which personal data is processed, as well as the relevant legal basis under Article 6 GDPR for each specific processing. Where special categories of data are processed, it should mention any relevant additional legal basis under Article 9 GDPR.

In addition, we assessed whether the controller linked each purpose to a specific legal basis and to specific categories of personal data. This requirement follows from the GDPR's transparency obligations⁸ and is supported by the European Data Protection Board (EDPB), which endorsed the guidelines on consent and on transparency of the Article 29 Working Party (WP29).⁹ It is actually also the only way for a user and a DPA to effectively assess and control whether the appropriate legal basis was used in the context of the controller's processing activities.

- **In case of "legitimate interests" as legal basis for processing: What are the interests of the controller or third parties?**

When the controller relies on legitimate interests as a legal basis for processing, it should inform the data subject about the interests and, at least upon request, provide data subjects with information on the balancing test. Controllers must carry out such a test whenever they rely on legitimate interests for processing and should communicate information on the balancing test in advance to the data subject.¹⁰

- **Recipients or categories of recipients of the personal data**

Recipients could be other controllers but also service providers. We expected the names of the recipients and the categories of personal data shared with each. At the very least, if for some reason

⁷ Article 29 Working Party "Guidelines on Data Protection Officers ("DPOs")", WP243 rev.01, p. 13.

⁸ Articles 5(1)(a), 12 GDPR.

⁹ Article 29 Working Party "Guidelines on consent under Regulation 2016/679", WP259 rev.01, p. 22 and "Guidelines on transparency under Regulation 2016/679", WP 260 rev.01, p. 8.

¹⁰ "Guidelines on transparency under Regulation 2016/679", WP 260 rev.01, p. 36.

not all recipients could be named, the controller should state the categories of recipients and indicated the activities they carry out, their industry, sector and sub-sector, and their location.¹¹

- **Transfers outside of the EU/EEA**

In case of data transfers to countries outside the EU/EEA, the countries should be named and the safeguards relied upon (e.g. adequacy decision under Article 45 GDPR, standard contractual clauses, derogations, etc.) should be specified. Also, the controller should provide for the means to access or obtain the relevant documents relating to the said safeguards.¹²

- **Retention periods**

The retention periods should be specific for the category of personal data concerned, or, at the very least, should allow the data subject for the assessment of the duration of data retention based on their own situation. If a controller provides that the data will be stored to comply with a legal obligation, it should specify which legal obligation it refers to.

- **Information about (selected) GDPR rights**

The controller should inform the data subject about their rights to access, rectification, erasure, restriction on processing, objection to processing, and portability, as well as the right to withdraw consent at any time and the right to lodge a complaint with a supervisory authority. Strictly speaking, it is not enough to merely inform about the existence of those rights, the controller should also include *“a summary of what each right involves and how the data subject can take steps to exercise it and any limitations on the right”*.¹³ This information about these rights should be brought to the attention of the individuals and presented clearly and separately from any other information.¹⁴ The right to lodge a complaint should explain that a complaint may be filed with the supervisory authority in a Member State of his or her habitual residence, their place of work or of an alleged infringement of the GDPR.¹⁵ Simply for the sake of brevity, we only assessed against the right to withdraw consent and the right to lodge a complaint with a supervisory authority.

- **Existence of automated decision making, including profiling; Meaningful information about the logic involved, as well as the significance and the envisaged consequences**

When the controller uses automated-decision making (including profiling), it should explain in clear and plain language how the profiling or automated decision-making process works. Additionally, the controller should inform about the significance and the consequences of such processing for the data subject.

All of the information elements are generally of equal importance.¹⁶

¹¹ Article 29 Working Party “Guidelines on transparency under Regulation 2016/679”, WP260 rev.01, p. 37.

¹² Article 29 Working Party “Guidelines on transparency under Regulation 2016/679”, WP260 rev.01, pp. 37-38.

¹³ Article 29 Working Party “Guidelines on transparency under Regulation 2016/679”, WP260 rev.01, p. 39.

¹⁴ Article 21 (4) GDPR.

¹⁵ Article 29 Working Party “Guidelines on transparency under Regulation 2016/679”, WP260 rev.01, p. 39.

¹⁶ Article 29 Working Party “Guidelines on transparency under Regulation 2016/679”, WP260 rev.01, p. 14.




2.1.2 Measurement criteria








































































Green ("mostly satisfactory") – the information is generally complete and provided in a concise, transparent, intelligible and easily accessible manner.

Yellow ("partly satisfactory") – the information is incomplete, vague, provided in a non-exhaustive manner or is misplaced (e.g. 'legal basis' mentioned in the 'purposes' section).

Red ("not satisfactory") – the evaluated element is missing or a contradictory statement is made (e.g. a privacy policy does not mention data transfers to third countries, even though the response to an access request acknowledges the existence of such transfers).

2.2 Overview of the selected information obligations under Article 13 GDPR

Symbols:  means mostly satisfactory.  means partly satisfactory.  means not satisfactory.

Information according to Article 13 GDPR	Zoom	Webex Meetings (Cisco)	GoToMeeting (LogMeIn)	Skype (Microsoft)	Teams (Microsoft)	Wire
Identity and contact details of the controller						
Contact details of the DPO						
Purposes of processing						
Legal basis for processing						
In case of legitimate interests: What are the interests of the controller or third parties?		Not applicable				
Interconnection: categories of personal data, purposes, and legal bases						
Recipients or categories of recipients of the personal data						
Transfers outside of the EU/EEA						
Retention periods						
GDPR right to withdraw the consent						
GDPR right to lodge a complaint						
Existence of automated decision making						

2.3 General observations: Poor structures and frequent changes

In general, the privacy policies suffer from similar weaknesses, ranging from poor structure and transparency to not being updated regularly. The policies we evaluated were in English and in effect as of 31.3.2020.

Privacy policies are typically living documents to reflect changes in processing activities. Zoom updated its privacy policy twice during our investigation, probably as a result of the increased media coverage and criticism it received over the last weeks.

Some companies update only selected country-versions of their policies and fail to keep them in sync. For example, Cisco's last updates range from April 2018 for Italy and Norway to December 2019 for the US.

Often, policies were poorly structured, overly long, or simply not user friendly, with information distributed in various places and not clearly linked or accessible straight from the main privacy policy.

For example, Microsoft refers users to their broad general privacy statement which, when downloaded in PDF, makes a 60-pages long document. It includes provisions on Skype, but contains almost no information at all on Teams. Zoom tries to shoehorn compliance with the various jurisdictions they operate in into one document. This may be efficient for the company, but it leaves the user with a disjointed reading experience that feels like a mixed buffet of competing flavours.

The next elements mention companies indicatively. The sections should not be read that the mentioned company is the only representative of the mentioned violation.

2.3.1 Controllership versus processorship

Most companies see themselves as processors and not as controllers in the context of their video conferencing service. This means that the user of the software would be the controller and could therefore be deemed responsible for compliance with the GDPR, which may indicate liability for any illegal processing by the processor.

Microsoft differentiates its role depending on whether the user is a private customer or a business, which is why for Teams it sees itself as a processor. Cisco does not make it clear what their relationship with the end user is. In their Webex Meetings Privacy Sheet, Cisco confirms that they process personal data in connection with the delivery of the Service, but *"if users participate in meetings hosted by users in other companies, the meeting host will control any meeting recordings or files shared during the meeting."*

The distinction is important. A controller is defined in Article 4(7) GDPR as *"the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data"*. In other words, a controller is the entity that decides how things get done. A processor, on the other hand, will typically be a service provider for the controller. As such, the processor has to follow the instructions given to it by the controller. As a general rule, it cannot do anything that it is not instructed to do.

The GDPR imposes a number of responsibilities on controllers *beyond* the information obligations investigated in this report, ranging from implementing appropriate technical and organisational security measures to choosing only such processors that provide sufficient guarantees.

It is important to note that the information obligations are only on the controller; they are not on the processor. It is contradictory when companies state that they are a processor and at the same time profess to comply with the GDPR requirements of controllers to provide information to their users.

It is beyond the scope of this report to assess in detail in which circumstances a video conferencing provider qualifies as a controller or/and a processor in the context of video conferencing. However, since we assume that such providers all qualify as controllers for at least a part of the processing operations involved¹⁷, we assessed the privacy policies against the standard of being a controller.

2.3.2 Privacy policies are too generic

Privacy policies should be concise, transparent, and easy to understand. In practice, privacy policies are often the opposite. They are riddled with broad language that only gives the appearance of providing real information.

For example, many policies state that they keep personal data “as long as necessary”, or that they “may share” personal data with third parties. Such empty phrases only give rise to further questions. How long is “necessary”? What does “may” mean – does the company share or does it not share personal data with third parties?

2.3.3 Missing link between categories of data, purposes of processing, and the legal basis for each purpose

Personal data should be collected and used for specific purposes. The controller collecting this data should specify the categories of processed data, the specific purposes it is intended for, and the specific legal basis they rely upon for each processing activity. For example, processing of a user’s bank account details (category of personal data) for payment of the services (purpose) is necessary for the performance of the contract (legal basis).

While companies mostly state general legal bases they rely on, they often fail to connect the categories of personal data to a specific legal basis and a specific purpose.

This is important because the user will have different rights depending on the legal basis used. For example, one right where consent is used as the legal basis is the right to withdraw the consent. This is not possible where a company relies on the legal basis of performance of a contract.

We found it hard to find any clear statement on the legal basis in the Webex Meetings (Cisco) privacy documents. In Cisco’s general privacy policy, the company includes a very general statement that they will “*retain and use your personal information as necessary to comply with our business requirements, legal obligations, resolve disputes, protect our assets, and enforce our agreements.*” Such a generic statement does not explain which categories of data are concerned. When compared with the Webex Meetings-specific privacy sheet, the legal basis is not mentioned at all. The information is limited to the categories of data and the purposes of processing.

¹⁷ See Recital 47 of the Directive 96/46 on the protection of individuals with regard to the processing of personal data and on the free movement of such data; see also Article 29 Working Party ‘Opinion 1/2010 on the notions of ‘controller’ and ‘processor’, WP 169, and in particular example provided p. 9.

2.3.4 In case of legitimate interests: the interests of the controller or third parties

Legitimate interests is a commonly relied upon legal basis. It often functions as a catch-all that companies rely on to justify processing that does not fall under the more common bases of consent or contractual necessity. However, because of the relative ease with which controllers can state their reliance on legitimate interests, they are required to not only state the interest, but, at least upon request, also provide information on the balancing test.

For example, Wire states that when purchases are made

“using a Team Admin account, Team Admins will be required to provide a payment method and may be required to provide additional account details, such as a billing address, phone number, email address and zip code if required for tax reasons or by the billing provider. Certain types of personal information relating to the specific transaction may also be collected, such as transaction amount and time. The legal basis for the processing of the data mentioned above is legitimate interest.”

Where data is legally required, such as for tax reasons, or is necessary for the purchase, other legal bases such as compliance with a legal obligation (Article 6(1)(c) GDPR) or necessity for the performance of the (billing) contract (Article 6(1)(b) GDPR) are likely to be more appropriate.

GoToMeeting (LogMeIn) and Zoom state that they may also receive information from other sources, including publicly available databases or from third parties from whom they have purchased data, and combine or “enrich” this data with information they already have. This third-party data collection is based on the companies’ “legitimate business interests”, which is often deemed to be for marketing purposes. In particular, when it comes to data collected from third parties, controllers should not rely on legitimate interests for marketing purposes. Such a combination of data from different sources without full transparency and awareness by the data subject is an undue intrusion upon their privacy.

2.3.5 Non-transparent data sharing / disclosure

All privacy policies mention that the companies (“may”) disclose personal data to other companies. Sharing personal data is not unusual or unlawful as such. It is often the case simply because not all companies do everything themselves. For example, just as a private consumer may decide to use a commercial email provider instead of hosting their own email server, a company may do so, too. Services can be of any nature, for example email hosting or the processing of credit card payments.

However, none of the companies are sufficiently transparent about their data sharing. Instead, they mask transparency in words like *may* or *might*, give overly broad descriptions of *service providers* or *vendors*, or include only examples of the recipients using the wording *such as*. Generally, controllers should name the recipients of personal data, as well as the purposes for the disclosure, and the location of the recipients.

One example of how not to report on the disclosure of data to third parties is the Webex Meetings Privacy Sheet. Cisco states that they “*may share*” some information with “*service providers, contractors or other third parties*”; “(t)he data shared *may include* aggregate statistics or pseudonymized data” (emphasis added). At first glance, the company mentions some hypothetical data sharing, but when looked at closely, the policy includes only empty phrases that do not give any

certainty to the reader, which is explicitly considered by the European Data Protection Board as poor practice.¹⁸

2.3.6 Inadequate information about data being transferred abroad

Transfers of personal data to a country outside the European Union (EU) or the European Economic Area (EEA) must follow special protection transfer mechanisms set out in the law. This is so that the high European level of data protection cannot be undermined by transferring personal data to a state that potentially has a lower level of data protection. Out of all the investigated policies, only Cisco's Webex Meetings Privacy Sheet provides an exhaustive list of destination countries. Other policies only state examples of destinations - theoretically, personal data *could* be sent to any country worldwide while leaving open the question of whether data was actually transferred or not.

While the global nature of the services means that international transfers will invariably take place when users are located outside the country where the services and servers are provided, policies can and should clearly explain and distinguish user-initiated transfers from other transfers that occur independently of where the user is located. Additionally, many policies only include an indicative listing of the legal mechanisms used for the transfer. Generally, companies merely repeat the relevant legal options under GDPR, without saying which option (if any) they actually use. This does not provide the user with any relevant information.

2.3.7 Unclear information about how long data is stored

Companies must inform their users for how long they store the personal data collected. Typical examples within Austria, where *noyb* is based, are the duration of the relevant statute of limitations (e.g. three years for civil claims, seven years for financial information). If it is impossible to provide the period, the criteria used to determine these periods may be provided instead.

If a company stores different categories of personal data for different periods of time, they should make it clear what this data is, why it is kept, and for how long the company intends to keep the data.

Out of the six video conference providers, only two provide acceptable information about how long the data is stored. Wire states the purposes of processing of selected categories of data and explains that the log data, for instance, is kept for a maximum duration of 72 hours, and customer data submitted in a support request will be kept for the duration of the resolution of the support case.

A perfect policy would also have stated the specific duration, i.e. years, required by law for mandatory storage. Mostly, privacy policies merely repeat the relevant legal provisions, vaguely stating that data is kept for as long as necessary to achieve the service's purposes, and provide non-exhaustive examples or retention periods for certain categories of personal data.

2.3.8 Misleading information about GDPR rights

We looked at two specific rights - the right to withdraw a consent and the right to lodge a complaint. The vast majority of the privacy policies list the rights of users in one way or another, though sometimes with the qualifier that users "may" have certain rights. This type of wording cannot be

¹⁸ Article 29 Working Party "Guidelines on transparency under Regulation 2016/679", WP260 rev.01, as endorsed by the EDPB, p. 8.

accepted and is definitively not in line with the GDPR, which intends to make clear to individuals that they are entitled to exercise different effective -and therefore not potential- rights.

In this context, Wire and Webex Meetings (Cisco) do not specify that users have a right to lodge a complaint with a supervisory authority - which is one of the most important rights under the GDPR since it provides an effective remedy to the individuals. The lack of such information might therefore create the impression that they are not entitled to have an effective remedy in front of a supervisory authority.

2.3.9 Name and contact details were mostly provided

Users must always be able to communicate with the companies that process their personal data in order to exercise their rights.

When there is an employee in charge of data protection matters, a so-called data protection officer or DPO, their contact details must also be published. Privacy policies generally provide contact information of a data protection officer, with the exception of Webex Meetings (Cisco). This may be because these companies consider that they do not fall under the duty to appoint a DPO, which was not part of this assessment.¹⁹ GoToMeeting (LogMeIn) provided contact details that apparently are both for the DPO as well as for “*questions about this privacy policy or our practices*”. Microsoft’s Skype and Teams failed to provide contact details; they only provided a web contact form as a method to contact the Microsoft Chief Privacy Officer or EU Data Protection Officer.

3. Conclusion

While the video quality of the investigated tools may often be crystal clear, and the user interfaces well-thought out, the service providers’ privacy policies do not meet this standard. Static in the form of “may” or “might”, “as necessary”, or “as required by law” cloud the picture. Sometimes whole parts are missing, such as information about basic GDPR rights. Finally, poor structure makes accessing the available information challenging. Video conferencing providers need to work on meeting their information obligations under the GDPR.

¹⁹ In this context, it should be reminded that the EDPB considers that the provision of telecommunication services constitutes a ‘regular and systematic monitoring of data subjects’ in the sense of Article 37 (1) a of the GDPR: see Article 29 Working Party “Guidelines on Data Protection Officers”, WP243 rev.01, as endorsed by the EDPB, p. 9.