Preliminary privacy assessment of Zoom as online conferencing tool

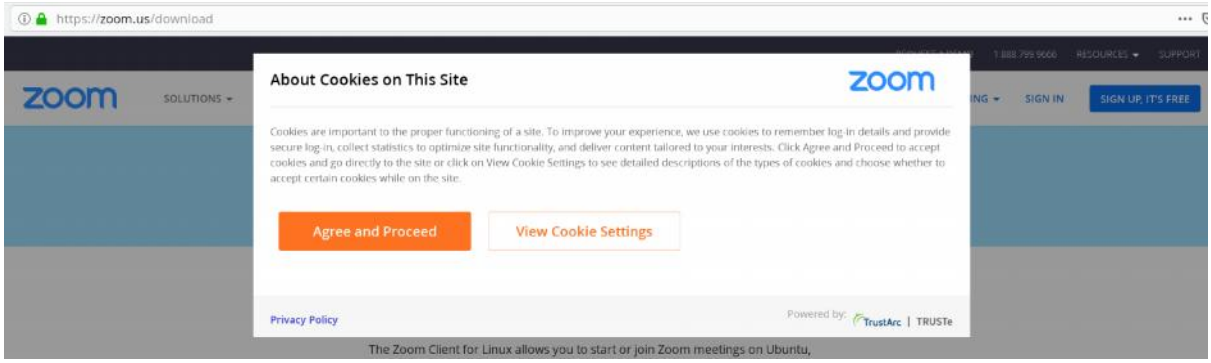
IT Policy Unit has been requested on 15 February a privacy assessment on two tools for podcasting with remotely connected speakers: Jitsi and Zoom.

IT Policy Unit sent a feasibility study on 21 February outlining the strong points and weaknesses of the tools proposed.

On 25 February IT Policy Unit was informed that the EDPS has contracted a "Pro" subscription plan of the service offered by Zoom. IT Policy Unit staff conducted some tests with the EDPS account.

Results of the tests

When joining a meeting using a URL provided by the organizer, the browser shows the participant a modal notice (cookie wall) with the available options.



Even before the participants has made any decisions, some cookies and HTML5 local storage are set on their devices. Some of those cookies (e.g. Google Analytics) are not exempted from the requirement to obtain previous informed consent.

This behaviour does not follow the recommendation 3 of the EDPS web services guidelines.

The default configuration ("Agree and proceed") is to accept all types of cookies which are classified as advertising, web functional and required). To limit the cookies to the required ones it is necessary to go into the option "View Cookie Settings".

This behaviour does not follow the recommendation 18 of the EDPS web services guidelines.

Google Analytics cookies are kept even if the participant limits the cookies to the required ones.

Current EDPS account of the Zoom service is set up so only local recording is allowed. Recording on the cloud service provided by Zoom is disabled.

Once the meeting has finished the service automatically starts the conversion of the collected data into a set of five files containing the video, audio and chat data of the meeting.

Using the user interface we could not found any recording or chat message related to previous test meetings.

Legal document assessment

This section contains a list of flaws detected on legal documents available at Zoom's website.

Privacy Policy

- The document does not make clear when Zoom acts as data controller or as data processor.

  The policy states that "*We may collect, either as Controller or Processor, the following categories of Personal Data about you when you use or otherwise interact with our Service:...*" and "*We collect and retain, generally as a Processor and in order to provide the Services, Personal Data and other information you upload, provide, or create while using the Service*"

- The EDPS should inform to all participants that, as the policy states: "*All messages and content you share in a meeting, including Personal Data about you or others, will be available to all other participants in that meeting.*".

- There is no information on the specific retention periods.

- The policy states that "If you use a feature of the Products that allows for Recordings (defined below), we collect information from you that you provide in connection with such use and through such Recordings, to the extent you provide it to us. This information may include Personal Data, if you provide us with Personal Data.". The policy further states that "Any person and/or entity who makes a Recording of a meeting or webinar shall be the data controller of that Recording, and Zoom will be the data processor with respect to the Recording.". It is clear that Zoom processes personal data in and related to recordings for their own purposes. They are not mere processor, but (joint) controllers for that processing.

- Zoom products do not support Do Not Track requests, which means that they collect information about visitors online activity both while they are using the Products and after they leave Zoom's websites.

  This behaviour does not follow the recommendation 23 of the EDPS web services guidelines.

Processing addedum

- The Processing addendum refers to compliance with Directive 95/46 and the GDPR.

- Use of sub-processors based outside of the EEA (mostly US), including in countries without an adequacy decision. Incomplete list of sub-processors[1] (e.g. Facebook, Google Analytics, PayPal...). Incoherence between provisions on sub-processors in the Processing addendum and the list of sub-processors, which limits the notification of the controller of any new sub-processors "*to the extent required under contractual agreement, along with posting such updates here*". This raises doubts on the compliance with Art. 29(2) of Regulation 2018/1725 (and Art. 28(2) of the GDPR), is the controller has not signed the Processing addendum with Zoom.

- EXHIBIT A. (Details of Processing) to the Processing addendum is not in line with the details provided for in the Privacy Policy document (e.g. types of personal data processed)

- EXHIBIT B. (Standard Contractual Clauses) to the Processing addendum is not in line with the details provided for in the Privacy Policy document (e.g. types of personal data processed).

[1] https://zoom.us/subprocessors

- Section 6 (Transfers of Personal Data) does not prohibit onwards transfers of personal data by the processor or sub-processors.
- Paragraph 7.1. of the Processing addendum limits the notification of the Controller of data subjects requests to the extent permitted by law. As the controller is the one ultimately responsible for fulfilling all controller's obligations (ensuring information and other data subject rights) and liable for any breach of those obligations. Therefore, in case the processor received and responds to data subject requests, the controller should be notified of the requests and the responses.
- Paragraph 8.1. of the Processing addendum states that the processor shall provide the controller with reasonable cooperation and assistance where necessary for Controller to comply with its obligations under the GDPR to conduct a data protection impact assessment and/or to demonstrate such compliance, provided that Controller does not otherwise have access to the relevant information. The assessment of that is reasonable is left to the processor. This limitation to what is reasonable is not in the GDPR (or Regulation 2018/1725).
- Paragraph 8.2. of the Processing addendum states that the processor shall provide the controller with reasonable cooperation and assistance with respect to Controller's cooperation and/or prior consultation with any Supervisory Authority, where necessary and where required by the GDPR. The assessment of that is reasonable is left to the processor. This limitation to what is reasonable is not in the GDPR (or Regulation 2018/1725).
- Paragraph 8.4. of the Processing addendum limits the controller's right to audit only to once per calendar year review of "*copies of certifications or reports demonstrating Processor's compliance with prevailing data security standards applicable to the Processing of Controller's Personal Data*".
- According to paragraph 8.5 of the Processing addendum in the event of a Personal Data Breach, Processor shall *"… take such steps as Processor in its sole discretion deems necessary and reasonable to remediate such violation (to the extent that remediation is within Processor's reasonable control)*". Thus, even though the controller is responsible for data breaches, it cannot give the processor any instruction on additional measures to mitigate the data breach if it deems that the measures taken by the processor are not enough. Paragraph 8.6. of the Processing addendum limits the cooperation and assistance to controller only to what is reasonable. The assessment of that is reasonable is left to the processor. This limitation to what is reasonable is not in the GDPR (or Regulation 2018/1725).

Cookie policy and consent management mechanism

- From this document, it is clear that Zoom is collecting data for their own purposes (e.g. for improving products and informing about Zoom's events and promotions and offers from third parties, personalised marketing communications). This collection of data using cookies and tracking technologies by Zoom and their third-party service providers is also set out in the privacy policy.
- There is no information on the duration of cookies and the retention period of the collected data.

Terms of service

- Section 3.c (Recordings) of the terms of service states that "You are responsible for compliance will all recording laws. The host can choose to record Zoom meetings and Webinars. By using the Services, you are giving Zoom consent to store recordings for any or all Zoom meetings or webinars that you join, if such recordings are stored in our systems. You will receive a notification (visual or otherwise) when recording is enabled. If you do not consent to being recorded, you can choose to leave the meeting or webinar.". Use of the Services is subject to Zoom's privacy policy. As privacy policy and other policies are incorporated into the Terms of service, by consenting to recording host and meeting participants are consenting to Zoom's processing of the personal data in and related to recordings for their own purposes.

  This can be mitigated by signing a separate written agreement with Zoom governing our use of the service, since in line with paragraph 20.3 (General provisions) of the terms of service such separate agreement would take precedence over Zoom's terms of service, privacy policy etc.