DPIA Zoom Education and Enterprise

SURF

Public version 1.3 25 February 2022

Colophon

DPIA by SURF

Kantoren Hoog Overborch (Hoog Catharijne)
3511 EP Utrecht
Moreelsepark 48

www.surf.nl

Contact Sandy Janssen
Sandy.janssen@surf.nl

Project name DPIA report data processing Zoom Meetings Enterprise 2022

Authors Privacy Company
Sjoera Nas and Floor Terra, senior advisors
www.privacycompany.eu

Version management

Version	Date	Summary of changes
0.1	10 September 2020	Outline part A
0.2	18 November 2020	Rough draft part A based on technical telemetry findings
0.3	15 December 2020	Added written answers Zoom and commitments made during conference calls on 4 and 11 December to part A.
0.4	18 December 2020	Feedback included from BZK about end-to-end encryption
0.5	21 December 2020	Comments SLM Rijk processed
0.6	2 April 2021	Comments Zoom on part A processed, version with track changes
0.7	2 April 2021	Clean version
0.8	14 May 2021	Input SLM and SURF processed with track changes
0.9	14 May 2021	Input SLM and SURF processed clean
1.0	17 May 2021	Complete first draft with track changes part A
1.1	18 May 2021	Complete first clean draft, shared with Zoom
1.2	9 February 2022	Revised and updated [part A of the] after negotiations with Zoom, input SURF processed
1.3	25 February 2022	Public version, input Zoom and SURF processed

CONTENTS

Overview of figures and tables

Summary

The Zoom Services allow people to make (video)calls, mute, and record calls, require passwords, require waiting rooms, download the chat sessions, add a profile picture or virtual background, share screens, touch up appearance, schedule and start meetings, invite participants from different domains and create a personal profile in the Zoom Account.

This Data Protection Impact Assessment (DPIA) examines the data processing via the paid services offered as Zoom Education and Enterprise, on five platforms:

- as installed app on Android and iOS devices
- as installed Zoom client for meetings on Windows 10 and MacOS, and:
- usage via the Zoom extension for the browser Chrome.

Additionally, this DPIA analyses the use of the Microsoft Outlook add-in and the usage of cookies and similar technology on the publicly accessible and restricted access Zoom website.

This report was commissioned by SURF, the organisation that procures ICT facilities for education and research institutions in the Netherlands. SURF took the lead in negotiations with Zoom after a first DPIA showed high risks. The initial DPIA was commissioned by the Strategic Vendor Management office for Microsoft, Google, and Amazon Web Services (SLM Rijk) of the Dutch government, together with the Ministry of the Interior and Kingdom Relations, and SURF.

Though SURF and the Dutch government have already negotiated a GDPR-compliant agreement with Microsoft for the use of Teams as a videoconferencing tool, they wish to assess via this DPIA what the risks are if universities and government organisations would deploy Zoom Meetings instead of, or next to, Microsoft Teams.

Personal data

This DPIA is based on a legal analysis of the available documentation about Zoom Meetings, answers from Zoom to detailed questions from Privacy Company and SURF, analysis of intercepted outgoing network and telemetry traffic from the tested apps, as well as an examination of the log files made available by Zoom to admins.

This report distinguishes between the following categories of personal data:

- Content Data
- Diagnostic Data
- Account Data end-users
- Account Holder Data (billing and sales contacts with Enterprise and Edu customers)
- Website Data
- Support Data
- Other Data: Feedback and Marketplace

Outcome: six low data protection risks

Initially, in May 2021, the outcomes of the DPIA showed nine high, and three low data protection risks. The measures Zoom had already taken, or announced, were not enough to mitigate these risks. The risks were mostly due to the fact Zoom did not provide any concrete plans and deadlines to mitigate the risks, and because Zoom and its Enterprise and Education customers factually qualified as joint controllers, and did not have a legal ground for the data processing.

After many conference calls and exchanges of information, SURF and Zoom have signed a new contract, a Data Processing Agreement (DPA) and an action plan with firm deadlines that mitigates all of the high risks. Zoom will apply most of these improvements to all of its EU Enterprise and Education customers, and make a new DPA publicly available.

The high risks have been mitigated as a result of the following measures and commitments:

1. Zoom is a US based company. **Many personal data are transferred by default to Zooms servers in the USA.** However, following a detailed Data Transfer Impact Assessment (DTIA) the risks for data subjects are negligible. Most importantly, since November 2020 Zoom offers end-to-end-encryption for all Content Data exchanged in Zoom meetings and webinars. Regardless of any legal or illegal pressure, Zoom is unable to provide access to the streaming Content Data in clear text/audio/video. Content Data and the service generated server logs are already generally processed within the EU, in the data centres nearest to the customer, but **Zoom has committed to process all personal data (Content, Account, Diagnostic, Support and the restricted access Website Data) exclusively in the EU for its EU Education and Enterprise customers, by the end of 2022**. Even earlier, by mid-2022, Zoom will offer European organisations the possibility to have all of their Support Data exclusively processed in the EU. In that case, organisations will have to provide consent if they wish to have their support requests processed outside of regular working hours, for transfer of the personal data outside of the EU. The only ongoing systematic transfer of personal data after the end of 2022 is the transfer of Diagnostic Data to Zoom's central Trust & Safety team in the USA, in case of a complaint or other type of abuse signal. All transfers are based on the new EU Standard Contractual Clauses (SCCs).

2. Zoom has agreed to become a data processor for all personal data, except for where authorised by controller and documented in the DPA to 'further' process some personal data as an independent controller, and in relation to its publicly accessible website. This was essential to solve many of the previous high data protection risks. As a data processor, Zoom is bound to strict purpose limitation. **Any processing of personal data for the purposes of marketing, profiling, research, analytics or (targeted) advertising is prohibited, as well as any 'compatible' or 'further' processing**, unless explicitly authorised in the DPA. This prohibition also applies to guest users that join a meeting organised by an EU Education or Enterprise customer. Zoom has agreed to a limitative list of purposes for which it is authorised to 'further' process some personal data, when strictly necessary for its own legitimate business purposes, as an independent data controller.

3. Zoom uses third parties for some data processing. Zoom has ensured that it has **subprocessor agreements with all of these parties**, has inventoried the subprocessors of its subprocessors and has ensured that **arrangements for onward transfers, such as SCCs, comply with the guarantees in the new DPA**. This also applies to the strictly necessary cookies set on Zoom's websites.

4. Zoom has **clarified and minimised the data retention periods**, to a maximum of 12 months for the different Account, Support and Diagnostic Data starting with the adoption of the new DPA by each customer. Zoom will create a possibility for admins to individually delete personal data before the end of 2022. Zoom is planning to anonymise IP-addresses from end users before storing these identifiers in a separate container, exclusively for fiscal compliance. Zoom is obliged to retain IP addresses for 6 years based on new US fiscal legislation. Zoom has become **more transparent about the Diagnostic Data** it processes. Zoom has already published a list of telemetry events it collects, and will steadily improve available public information about all Diagnostic Data. Zoom has published an updated Cookie Policy.

5. Zoom has committed to **develop self-service tools for administrators and for end users to file Data Subject Requests** before the end of 2022, as well as a take-out for admin behaviour. Pending the realisation of these self-service tools, Zoom has committed to manually provide complete access in reply to data subject requests.

6. Zoom has taken many steps to **comply with the privacy by design and privacy by default principles**, for example by disabling by default the Feedback functionality (thumbs up/thumbs down after every conversation), and by only setting/reading strictly necessary cookies on its websites by default. Zoom has contractually committed never to ask Enterprise and Education account end users for consent for new features. Only the admin is able to enable new data processing, with an active opt-in.

7. Like all other cloud providers Zoom is **obliged under US law to report confirmed Child Sexual Abuse Material (CSAM)** to an NGO in the United States (NCMEC). Zoom has mitigated the risks of such an onward transfer by only reporting exact matches with known material, **after human review**. Zoom will follow future EDPB guidance on this topic.

8. Zoom has agreed **not to send any unsolicited commercial communications to admin and end user Account Data**, only to its commercial contacts (Sales Managers). Zoom will develop a marketing preferences self-service tool for all Account owners by the end of 2022.

Overview of six low risks and mitigating measures

No.	6 low risks	Measures gov orgs and universities	Measures Zoom
1.	Transfer of Content Data to the USA	Apply E2EE to all Meetings. Warn users that E2EE is not possible in browser	Comply with the privacy guarantees in the SCCs, inform SURF when compliance is no longer possible
		If E2EE is not applied: choose the EU as Content Storage Location setting. Consider local recording instead of cloud recording	
		Complete the model DTIA to assess the risks of unlawful access/disclosure of sensitive/ special/secret categories of personal data processed by Zoom	Apply the contractually guaranteed human review after a match with known CSAM, allow end users to appeal to a decision to terminate their account
		Enable 'EU-only' for Support requests as soon as Zoom offers this option. Draft an instruction for admins when they can consent to export of	Organise an independent ISO and SOC-2 audit every year or two years: allow SURF and the central

		Support data to third countries in exceptional circumstances	Dutch government to add one specific audit question every year
		Consider use of the available privacy options such as: • Enable advanced chat encryption • Prevent participants from saving chats • Mute individual or all participants upon entry • Turn off file transfer • Turn off annotation • Disable private chat • Turn off screen sharing for participants • Prohibit the (local) recording of video during screen sharing • Prohibit the viewing and recording of the 'gallery' during screen sharing	Publish as much details as possible in the bi-annual transparency reports
		Only use Webinars for non-confidential, non-sensitive public data (no E2EE)	Update the DTIA if necessary, following guidance from the EDPB
		Create policy rules to prohibit the use of directly identifying personal or confidential data in room and topic names. Do not use labels to categorise users. Perhaps, in some circumstances, instruct users not to use profile pictures	
2.	Transfer of Account, Diagnostic, Support and Website Data to the USA (until end of 2022)	Consider the use of SSO with pseudonymous identifiers for employees whose identity must remain confidential. If end users are allowed to individually sign-up: tell them the consumer privacy policy and TOS do **not** apply.	Realise a general rule of personal data processing in the EU by the end of 2022, all exceptions to be approved by SURF.
			Update the DTIA if necessary, follow guidance from the EDPB
		Use a Vanity URL to prevent the transfer of IP addresses when end users sign in, and to prevent that end users visit Zoom's publicly accessible website hosted in the USA	Publish as much details as possible in the bi-annual transparency reports
		Do not use the default mail provider Twilio to send invitations for Webinars: use own EU-based mailing provider	Remove traffic to the US Consent Manager from the "restricted access website" located in the EU, to prevent transfer of personal data to the USA
3.	Transfer of pseudonymous Diagnostic Data to the USA Trust & Safety team (ongoing)	Follow guidance from SURF and the EDPB if this risk can be accepted, as calculated in the DTIA	Update the DTIA if necessary, follow guidance from the EDPB
			Consider shortening the retention period of 180 days
			Consider creation of a second Trust & Safety Team in the EU for EU customers

4.	Lack of transparency Account and Diagnostic Data	Study current and future Zoom documentation: inform end-users about the contractual privacy guarantees for the processing	Publish centrally accessible, exhaustive, and comprehensible documentation about the different types of Diagnostic Data, keep the new documentation up to date
		As soon as Zoom makes this possible: show organisation's own privacy conditions for the use of Zoom during sign-up.	
5.	Difficulty to exercise Data Subject Access Requests	Regularly use new access tools when Zoom makes those available: to honour individual requests from employees/students, and as admins, to check compliance with public documentation	Build the agreed improved access-tool for admins to take-out all personal data per end user [by the end of 2022]
			Create a self-service access tool for end users [by the end of 2022]
		Inform employees how they can access their personal data in the available admin log files and reports	Until completion of the self-service tools: provide complete and timely answers to data subject access requests
6.	Employee monitoring system	Create a policy to prevent use of audit logs and reports as an employee monitoring tool	Develop an easier take-out for log files of admin behaviour [by the end of 2022]
		Regular check the logfiles with admin behaviour to verify compliance	

Conclusions

If and when Zoom and the Dutch universities and government organisations apply all the agreed and recommended measures, there are no known high risks for the individual users of the Zoom videoconferencing services.

Caveat. It is uncertain how the transfer risks will be assessed by the national data protection authorities, in their joint investigation into the use of cloud services by public sector organisations. The results are expected by the end of 2022. For this DPIA the transfer risks have been rigorously assessed, including a separate DTIA. Zoom has committed to follow recommendations from the EDPB, and to loyally collaborate with SURF and the Dutch government to update the DTIA when necessary.

Introduction

This report was originally commissioned by the Strategic Vendor Management office for Microsoft, Google, and Amazon Web Services (SLM Rijk[1]) of the Ministry of Justice and Security, together with the Ministry of the Interior and Kingdom Relations, and SURF, the organisation that procures ICT facilities for education and research institutions in the Netherlands. After an initial version was provided to Zoom, SURF took the lead and commissioned this updated report with the outcomes of the negotiations with Zoom. This DPIA examines the data processing via the paid services offered to EU customers with Education and Business/Enterprise licenses.

Zoom describes its own services as: "*Zoom Meetings Services enable Hosts to schedule and start Meetings and to allow Participants to join Meetings for the purpose of collaborating using voice, video, and screensharing functionality. Every meeting will have at least one Host. Chat features allow for out-of-session one-on-one or group collaboration.*"[2]

Previously, SLM Rijk and SURF have collaborated in negotiations with Microsoft about different Microsoft Office 365 and Windows 10 products and services[3], and about Google Workspace for Education and Enterprise.[4] The full reports with appendices are available in English, with a brief summary in Dutch. The DPIA reports have been written by the Dutch privacy consultancy firm Privacy Company.[5]

DPIA

Under the terms of the General Data Protection Regulation (GDPR), an organisation is obliged to conduct a data protection impact assessment (DPIA) under certain circumstances, for instance where it involves large-scale processing of personal data. The assessment is intended to shed light on, among other things, the specific processing activities, the inherent risk to data subjects, and the safeguards applied to mitigate these risks. The purpose of a DPIA is to ensure that any risks attached to the process in question are mapped and assessed, and that adequate safeguards have been implemented to mitigate those risks.

According to the GDPR a DPIA assesses the risks for the rights and freedoms of individuals. Data subjects have a fundamental right to protection of their personal data and some other fundamental freedoms that can be affected by the processing of personal data, such as for example freedom of expression.

The right to data protection is therefore broader than the right to privacy. Recital 4 of the GDPR explains: "*This Regulation respects all fundamental rights and observes the freedoms and principles recognised in the Charter as enshrined in the Treaties, in particular the respect for private and family*

[1] SLM is the abbreviation of the Dutch words: Strategisch Leveranciers Management.

[2] Zoom Services Description, 8 December 2020, URL: https://zoom.us/docs/en-us/services-description.html.

[3] SLM Rijk, overview of published DPIAs, URL: https://slmmicrosoftrijk.nl/downloads-dpias/.

[4] SURF, Google Workspace for Education support package, URL: https://www.surf.nl/en/news/google-workspace-for-education-support-package.

[5] Privacy Company, URL: https://www.privacycompany.eu/.

life, home and communications, the protection of personal data, freedom of thought, conscience and religion, freedom of expression and information, freedom to conduct a business, the right to an effective remedy and to a fair trial, and cultural, religious and linguistic diversity."

This DPIA follows the structure of the DPIA Model mandatory for all Dutch government organisations, with some small adaptations to make the model more suitable to analyse the specific risks caused by the use of a cloud service provider.[6]

Umbrella DPIA versus individual DPIAs

Though the Dutch government and SURF have already negotiated a GDPR-compliant agreement with Microsoft for the use of Teams as a videoconferencing tool, they wish to assess via this DPIA what the risks are if universities and government organisations would deploy Zoom Meetings instead of, or next to, Microsoft Teams.

Pursuant to Article 35 GDPR, data controllers are obliged to conduct a DPIA if the processing meets two, and perhaps three of the nine criteria set by the European Data Protection Board (EDPB), or if it is included in the list of criteria when a DPIA is mandatory in the Netherlands.[7]

If Dutch organisations would use Zoom Enterprise services, this would involve processing of data from and about the communication (content and metadata). Because Zoom Enterprise is a cloud service, it is inevitable that Zoom processes personal data about the behaviour of employees, administrators and other people participating in the video calls.

Criteria EDPB

The circumstances of the data processing via Zoom Meetings meet three out of the nine criteria defined by the EDPB:

- Sensitive data or data of a highly personal nature (criterion 4). The EDPB explains: "some categories of data can be considered as increasing the possible risk to the rights and freedoms of individuals. These personal data are considered as sensitive (as this term is commonly understood) because they are linked to household and private activities (such as electronic communications whose confidentiality should be protected)."
- While the Zoom Services are neither designed, nor marketed as a tool for behaviour monitoring, there is a possibility that the processing operations (via the Zoom cloud log files and through the audit logs for system operators) lead to a systematic observation of the behaviour of employees, especially since the pandemic lead to a massive increase in the use of videoconferencing tools (criterion 3);
- The processing involves data relating to vulnerable data subjects (criterion 7). Both employees and other data subjects whose personal data are processed through the Zoom Enterprise

[6] *Model Gegevensbeschermingseffectbeoordeling Rijksdienst (PIA)* (September 2017). For an explanation and examples (in Dutch) see: https://www.rijksoverheid.nl/documenten/rapporten/2017/09/29/model-gegevensbeschermingseffectbeoordeling-rijksdienst-pia.

[7] Dutch DPA, (in Dutch only), list of DPIA criteria published in the Staatscourant (Dutch Government Gazette) of 27 November 2019 , URL: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/stcrt-2019-64418.pdf.

services are in an unequal relationship of power with the universities and government organisations, including for example job applicants).[8]

- Apart from that, in their Opinion on data processing at work, the European Data Protection Authorities (EU DPAs) recommend that organisations conduct a DPIA before using "*office applications provided as cloud service, which in theory allow for very detailed logging of the activities of employees*."[9]

The EU DPAs mention work applications as one of the eight relevant monitoring technologies and write: "*Irrespective of the technology concerned or the capabilities it possesses, the legal basis of Article 7(f)* [since replaced by GDPR art. 6(1) f, addition by the authors] *is only available if the processing meets certain conditions. Firstly, employers utilizing these products and applications must consider the proportionality of the measures they are implementing, and whether any additional actions can be taken to mitigate or reduce the scale and impact of the data processing. As an example of good practice, this consideration could be undertaken via a DPIA prior to the introduction of any monitoring technology.*"[10]

Criteria Dutch Data Protection Authority

The Dutch Data Protection Authority mentions the processing of communication data as specific criterion when a DPIA is mandatory:

"*Communication data (criterion 13). Large-scale processing and/or systematic monitoring of communication data including metadata identifiable to natural persons, unless and as far as this is necessary to protect the integrity and security of the network and the service of the provider involved or the end user's terminal equipment.*"[11]

This criterion may apply to the Zoom Enterprise services, as the monitoring of communication data could be necessary to protect the integrity and security of the network. However, in order to be able to assess the impact of the data processing and to determine whether the actual processing meets the requirement of necessity, the government organisations must first conduct a DPIA (or have it carried out). This DPIA examines the necessity for Zoom to collect and store the communication data, as well as the necessity and circumstances in which the employer can use these communications data.

In GDPR terms, SURF and SLM Rijk are **not the data controllers** for the processing of personal data via the use of the Zoom Enterprise services. However, as central negotiator for many cloud services, they commission this DPIA in acceptance of their legal responsibility to assess the data protection risks for the employees and negotiate for a framework contract. Therefore, this umbrella DPIA is meant to assist universities and government organisations to select a privacy-compliant deployment. They can rely on the technical and legal analysis in this report, but this report cannot entirely replace a specific

[8] EDPB adopted Guidelines on Data Protection Impact Assessment (DPIA) (wp248rev.01), 13 October 2017, URL: http://ec.europa.eu/newsroom/document.cfm?doc_id=47711.

[9] Article 29 Working Party, WP 249, Opinion 2/2017 on data processing at work, 23 June 2017, p. 13, URL: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610169.

[10] Idem, p. 14.

[11] Dutch DPA, (in Dutch only), list of DPIA criteria published in the Staatscourant (Dutch Government Gazette) of 27 November 2019.

DPIA, in which the organisation itself assesses the specific data protection risks, related to the technical privacy settings, nature and volume of the personal data it processes and the vulnerability of the data subjects.

This umbrella DPIA thus cannot replace the specific risk assessments the individual universities and government organisations must make themselves.

Different Zoom Meetings editions

Zoom provides both free and paid videoconferencing services, in four different price plans: Free, Pro, Business and Enterprise.[12] For this DPIA, the Enterprise version was tested. Additionally, Zoom has an offer for schools and universities called Zoom for Education. Privacy Company did not test the actual data processing in a Zoom for Education *tenant*. However, Zoom explained that in principle, the Enterprise and Education versions were identical in data processing at the time of this investigation[13], except for certain default settings (stricter in the Education license) and some different contractual guarantees. Where relevant, these differences are mentioned in this DPIA.

A key data protection difference between the free Basic Zoom application and Zoom Enterprise is that Zoom Enterprise offers advanced administration controls and the capacity to organise Webinars.

Scope of this DPIA: Zoom Education and Zoom Enterprise

This DPIA is focused on the processing of personal data through Zoom Meetings for professional users, not for consumers.

This DPIA examines the risks of the use of Zoom Meetings on five platforms:

- as installed app on Android and iOS devices
- as installed Zoom client for meetings on Windows 10 and MacOS, and:
- usage via the Zoom extension for the browser Chrome.

Additionally, the following two extra services and topics were tested with scripted scenarios:

- Microsoft Outlook add-in
- Usage of cookies and similar technology on the publicly accessible website, also after log-in (the restricted access Zoom portal)

All tested scripts contain a selection of representative user actions in the different Zoom services: scheduling and making video and (separate) audio calls, inviting participants in the same organisation, inviting guests from outside the organisation, adding virtual backgrounds and profile pictures, sending private messages, sending channel messages, and creating and using a private room.

In principle the default settings were followed with regard to privacy and security options. However, Privacy Company also tested the difference when privacy friendly options were enabled:

- Make use of waiting room mandatory for all participants

[12] Zoom, Choose a plan, URL: https://zoom.us/pricing.

[13] Zoom commented in reply to the Zoom DPIA that there is no contractual guarantee that they remain identical, as the product is subject to rapid development.

- Prohibit recording
- Prohibit downloading
- Prohibit the use of Marketplace apps

Where possible, additional functionalities were used in combination with the videoconferencing facilities. Privacy Company tested the following extra services/features:

- Downloading chatlogs by meeting participants
- Recording a meeting
- Creating and participating in a poll
- Changing profile information (incl. user image)
- Using virtual backgrounds
- Using the "touch up my appearance" feature
- Using waiting rooms
- Screen sharing
- Muting call participants
- Inviting external users to a meeting

The default privacy settings for these options are described in Section 3.1 of this DPIA report.

Out of scope

This DPIA does not examine the data protection risks of:

- Zoom Phone
- Zoom Rooms for Conference Rooms[14]
- Zoom Video Webinars[15]
- Zoom App Marketplace. Apps such as Slack, LinkedIn, Teams and Gmail can be embedded with Zoom. This DPIA has only tested the possibility for admins to disable access to the Marketplace.

Methodology

This DPIA is based on multiple sources of information. Privacy Company combined a legal fact-finding strategy with a technical examination of the data processed through the use of Zoom Enterprise.

[14] Both Zoom Phone and Zoom Rooms are listed by Zoom as Zoom Professional Services, URL: https://zoom.us/docs/doc/Zoom_Professional_Services_Overview.pdf.

[15] Zoom's Enterprise and Education licenses included limited use of Webinar functionality: up to 500, resp. 1.000 participants. The data processing by this Webinar functionality was not separately tested, but is covered by the new Data Processing Agreement with Zoom.

Legal fact-finding

Privacy Company carefully reviewed all available public documentation from Zoom about Zoom Meetings, including all relevant contractual documentation for EU Zoom Enterprise customers.

Privacy Company asked questions and engaged in an ongoing dialogue with representatives of Zoom, initially with SLM Rijk, and after May 2021, with SURF.

Privacy Company filed a Data Subject Access Request (DSAR) on 12 October 2020 for the two test accounts, and exchanged a number of e-mails with Zoom about the results between 23 October and 20 November 2020. On behalf of Privacy Company, the Ministry of Justice and Security sent a letter with legal questions to Zoom on 20 October 2020. Zoom answered on 23 November 2020. To better understand Zoom's answers, and to discuss possible improvement measures, two conference calls were held between Zoom, SLM Rijk and Privacy Company, on 4 and 11 December 2020.

In March 2021, Zoom replied to the factual findings. In May, the first DPIA was completed and shared with Zoom. SURF, Zoom and Privacy Company have engaged in many meetings and exchanges after the summer of 2021.

Technical fact-finding: log files, traffic interception and DSARs

Because Zoom Meetings is a remote, cloud-based service, data processing takes place on Zoom's cloud servers. As a result, it is not possible to inspect via traffic interception how Zoom processes Diagnostic Data in its system generated logs about the use of the Zoom account and the Zoom services.

As described in more detail in Appendix 1 with this report (*Technical analysis Zoom Enterprise*), it is possible to gain insights in the personal data Zoom generates and processes about the use of its cloud services in three distinct ways:

1. Accessing admin log files
2. Interception of outgoing data traffic
3. Filing of Data Subject Access Requests (DSARs)

It is possible to inspect the log files Zoom makes available to administrators about interactions from end users with its cloud servers and compare these results to the input provided through the scripted test scenarios.

The executed scripts contain a selection of representative end user actions in Zoom Meetings as they could be performed by an employee of a Dutch government organisation. The scenarios were executed on 30 September 2020 (iOS, macOS, Windows and Android apps).

Initially, Privacy Company was erroneously provided with a 'free' test account by Zoom. This account did not give access to the audit logs. On 21 October 2020 Zoom changed the type of subscription to a paid Enterprise account. This enabled Privacy Company to export the available historical operational logs from the administrator console that contained information about the activities performed by the two test accounts prior to the export. See Section 3.1.1 for a detailed description of the contents of the available reports and logs.

Additionally, Privacy Company intercepted the data traffic from the end-user test devices. When Zoom collects information from the end-user device (such as Telemetry Data), the contents of this traffic

can sometimes be decoded. Furthermore, conclusions can be drawn about the network endpoints of traffic from end-user devices. Privacy Company saved the captured files and compared the network endpoints with the limited information published by Zoom about this topic. These results are described in Section 2.3 of this report and in Appendix 1 to this report.

Privacy Company intercepted the outgoing data with software that makes it possible to inspect the content of traffic with and without TLS encryption, Mitmproxy version 5.0.1 and Wireshark (the latter only for iOS).

The Mitmproxy was used as follows:

- Configure the laptop or phone to use the proxy
- Start the Mitmproxy
- Launch the specific mobile application
- Log in with a Zoom administrator, licensed user, or guest account as needed
- Run the scripted scenario. Make screenshots of each step.
- Once the script is fully executed, stop the Mitmproxy.

Because the Telemetry Data initially could not be intercepted in a legible form, the test scenarios on the Android and iOS apps were repeated on 10 November 2020. In spite of Zoom's public documentation about an in-built possibility for admins to work around the certificate pinning in both apps, this option initially did not work, nor in the Android, nor in the iOS app. Zoom explained on 15 October 2020 that it was possible to intercept the iOS app traffic with Intune MDM, but this solution did not work on Android, nor did it work as specified for iOS. See Appendix 1 with the technical investigation results for a more detailed explanation.

As a third method to compare the input from the executed test scenarios with the data stored by Zoom as a data controller, on 12 October 2020 Privacy Company filed two formal GDPR Data Subject Access Requests (DSARs) with Zoom, requesting access and a copy of the personal data relating to the two test accounts. Zoom initially responded the same day with a reference to its publicly available information, and the console for system administrators.

On 13 November 2020 Zoom replied more substantially to the access requests. These results are described in Section 2.4 of this report. The complete answer is appended in Appendix 1 to this report.

Privacy Company tested the software on the different platforms with the then most up to date versions, plug-in, and Chrome browser.

Table 1: Tested app versions per operating system

Operating system	Zoom client or app first test run	Zoom app second test run
MacOS version 10.15.7	5.3.1 (52877.0927)	
Windows Pro 19041.508	5.3.1 (52879.0927)	
Android OS Versie 9, 5 September 2020	5.3.52640.0920	5.4.2.524
iOS 12.3.1	5.3.0	5.4.1

Windows 10 Pro 19041.508	Chrome version 85.0.4183.121 Zoom extension version 1.5.9	
Windows 10 Pro 19041.508	Outlook version 2008 build 13127.20408 (*Click and Run*) App version 5.3.52819.0925	

Privacy Company ensured the research is reproducible and repeatable. This was achieved by working with written scenarios in which the number of actions is limited. There was a pause of 30 seconds between each action. Screenshots were taken of all actions. All data have been recorded.

Summary of previous mitigating measures Zoom

Since the start of this DPIA, Zoom has improved its GDPR compliance through many product innovations. At the end of January 2021, Zoom created a new option for EU system administrators of Enterprise and Education licenses to store a subset of Content Data only in the EU (in Germany). This geolocation choice only applies to cloud recordings, meeting transcripts, in-meeting chat messages and files exchanged in-meeting via chat, plus the service generated server logs and the back-ups. This choice was (and is) not (yet) available for other Content Data, such as the Account Data, including imported contact and calendar data, and contents of Support Requests.

Zoom's specific response to part A of the initial DPIA (the factual findings) can be summarised with the following two main inputs:

- Zoom insisted on a role as data controller for most of the Diagnostic Data and the Support Data. Zoom only changed its position for the Account Data, from an initial self-qualification as data controller to a role as data processor. Zoom saw itself in a complicated double role as processor and as controller for the different categories of Diagnostic Data. Zoom did not accept a role as joint controller with its Enterprise and Edu customers for these Diagnostic and Support Data.[16]
- Zoom committed to becoming more transparent about the data processing and provided a privacy sheet with a description of its role per category of personal data, a description of the purpose(s) and the legal ground. However, Zoom did not provide a timeline or specific text proposals, and could not guarantee all planned improvements and new documentation would be available before the DPIA was completed. The sheet did not include the Website Data.

The new information about the categories of personal data and purposes was added to the first DPIA (May 2021).

In reply to the first DPIA Zoom committed to take the following mitigating measures:

- Only process the Account Data and some of the Diagnostic Data as data processor and modify the enrolment framework accordingly

[16] Zoom reply to part A of the DPIA, separate table with the categories of personal data, Zoom's role, and legal ground, 19 March 2021.

- Work on a method to ensure that guests, when they use their free consumer account, are protected under the negotiated data protection guarantees for the Dutch universities and government organisations
- Become more transparent: publish a Privacy Data Sheet with detailed information about the different kinds of personal data it collects (except Website Data) and improve the information in other relevant public documentation
- Add omitted categories of personal data to the Privacy Data Sheet
- Stop using tracking cookies by default on its restricted access web pages (Portal)
- Provide explanations about measures admin can already take to mitigate some transfer risks, such as the use of a vanity subdomain
- Improve the DSAR process to immediately provide the relevant personal data (including the Telemetry Data, but not the Website or Cookie Data)
- Make it easier for admins to take out all data relating to one particular data subject
- Stop collecting the unencrypted Passcode in the audit log files
- Investigate the possibility of contractually and technically excluding the use of Microsoft's PhotoDNA for the Enterprise and Edu customers

However, these measures were not enough. The initial DPIA showed nine high, and three low data protection risks. Zoom's measures were not enough to mitigate these risks. The risks were mostly due to the fact that Zoom did not provide any concrete plans and deadlines to mitigate the risks, and because Zoom and its Enterprise and Education customers factually qualified as joint controllers, and did not have a legal ground for the data processing.

Table 2: Overview of initial high risks and mitigating measures (May 2021)

9 high risks	Measures gov orgs and universities	Measures Zoom
Lack of purpose limitation Content Data	Agree on contractual purpose limitation	Become a data processor for all Content Data and Account Data of end users, including guest users. Amend contract to provide limitative list of specific and explicit purposes for the processing of specific data
		Stop using PhotoDNA, or similar tools to proactively scan contents for illegal content/child abuse. If such scanning is no longer prohibited in the EU, give admins control
		Exclude data processing for any marketing communication, profiling, research, analytics or (targeted) advertising purpose
		Exclude 'compatible' or 'further' processing
		Amend contract to include exhaustive list of legitimate business purposes, when Zoom may act as data controller
Lack of purpose limitation Diagnostic, Support, Website and Feedback Data	Use SSO with a vanity subdomain to prevent users from having to use the Zoom website. Consider the use of pseudonymous identifiers, instead of email addresses	Become a data processor for all metadata, also from guest users. Amend contract to provide limitative list of specific and explicit purposes for the processing of specific data, only when proportionate.

	Create policy rules to prohibit the use of directly identifying personal or confidential data in room and topic names and in user categorizations. Perhaps, in some circumstances, instruct users not to use profile pictures	Exclude data processing for any marketing, profiling, research, analytics or (targeted) advertising purposes
	Use admin controls to prevent storing of Content Data when Zoom offers such options	Define when anonymisation of specific personal data for specific purposes is permitted, and commit to comply with EDPB guidance on anonymisation
	Create policy rules that hosts should not turn on the Feedback option	Exclude catch-all purposes such as compatible purposes, or asking for consent for any new purpose
	Warn users not to input personal data in the open text field in the Feedback form.	Amend contract to include exhaustive list of legitimate business purposes, when Zoom may act as data controller
Lack of transparency Diagnostic, Support, Website and Feedback Data	Study metadata documentation when it becomes available: inform end-users about the contractual privacy guarantees for the processing	Publish centrally accessible exhaustive and comprehensible documentation about the types of data, contents and purposes for processing of the different kinds of Diagnostic, Support and Feedback Data. Include missing user-provided Content Data
	Regularly use new access tools when Zoom makes those available: to honour individual DSARs and to check compliance with contract	Provide access to admins to all metadata: improve online take-out tool all personal data per end user
		Create a tool for end users and admins to view the Telemetry Data
		Comply with the legal transparency requirements about cookies and similar technologies (improve explanation in Cookie Consent Manager, improve Cookie Policy).
Lack of transparency about the Account and Feedback Content Data	Use SSO to prevent end users from having to accept the general Privacy Policy and Terms of Service.	Change the onboarding procedure for Enterprise and Edu customers: do not ask for date of birth, do not force acceptance of consumer legal texts, strongly encourage the use of SSO and a vanity subdomain.
	Inform end users about the contractual privacy guarantees for the processing, assure that they are not 'consenting' to the use of their Account Data for commercial purposes	
	Warn users not to input personal data in the open text field in the Feedback form.	Give a clear warning to end users in the Feedback form that they should not provide personal data
		Explain that both admins and Zoom have access to the Feedback Data (but only process meta and Content Data as data processor)
No legal ground for Zoom and gov. orgs/universities as joint controllers	Do not use Zoom Meetings until the processing can be based on one or more legal grounds	Become a data processor and process only for authorised purposes, so universities and government organisations can successfully invoke the legal grounds of contract, public and legitimate interest
		Alternatively: enter into a joint controller agreement
		Comply with the Dutch telecommunications Act with regard to the collection of Telemetry and Website Data, stop scanning Content Data to proactively detect illegal content

		Amend contract to include exhaustive list of legitimate business purposes, when Zoom may act as data controller
		Create more legal barriers against disclosure to law enforcement authorities to prevent violation of art 48 of the GDPR (contest validity of orders, always inform customer unless gagging order)
Privacy unfriendly default settings on the Website	Use SSO to prevent end users from having to accept tracking cookies on the Product pages.	Change the default setting on Product Pages to 'required cookies,' and remove tracking cookie
	Use a vanity subdomain, and copy all relevant documentation, including legal texts, to this subdomain	Change the default setting on the Marketing Pages to functional cookies, and comply with the Dutch telecommunications Act
		Comply with the legal transparency requirements about cookies and similar technologies (improve explanation in Cookie Consent Manager, improve Cookie Policy).
Missing privacy controls for admins	Use controls when they become available	Create central controls for admins to: ● Limit the collection of Telemetry Data and other Diagnostic Data ● Prohibit some of the purposes for Content and Diagnostic Data; ● Enforce data protection and security settings for guest users ● Prevent participants from saving chats ● Mute individual or all participants upon entry ● Turn off file transfer ● Turn off annotation ● Disable private chat ● Turn off screen sharing for participants ● Prohibit the recording of video during screen sharing
	Create policy rules for hosts to use these controls per meeting, when appropriate	
Lack of control subprocessors Diagnostic, Support, Website and Feedback Data		Become data processor for the processing of all personal data
		Stop using third parties to process metadata unless authorised as subprocessor
		Extend the period of 15 days to allow customers to meaningfully object against new subprocessors
Inability to exercise data subjects access rights	Inform employees about access to the data in the available admin log files and reports	Honour data subject access rights, including with respect to all personal data in the Content, Account and metadata.
		Develop an improved access tool for admins to allow data subjects access to all personal data.
		Accept additional identification from end users to grant access to webserver access logs and cookie information
	When available, use the improved take-out tool or (if joint controllers), inform users how to exercise their rights with Zoom	Develop a self-service online DSAR tool for end-users (including guest users)

New commitments and improvements Zoom after the first DPIA

After the summer of 2021, having studied the first DPIA, Zoom changed its approach. Zoom committed to mitigate all high risks. After many open-minded conference calls and exchanges of information, SURF and Zoom have signed a new contract, a Data Processing Agreement (DPA) and an action plan

with firm deadlines that mitigates all of the high risks. Zoom will apply most of these improvements to all of its EU Enterprise and Education customers, and make a new DPA publicly available.

Outline

This assessment follows the structure of the *Model Gegevensbeschermingseffectbeoordeling Rijksdienst (PIA)* (September 2017).[17] This model uses a structure of four main sections, which are reflected here as "parts".

A. Description of the factual data processing
B. Assessment of the lawfulness of the data processing
C. Assessment of the risks for data subjects
D. Description of mitigation measures

Part A explains the data processing by Zoom of the Meeting Services on the different platforms (as desktop and mobile apps and web based, accessed via a Chrome Browser and as a plug-in for Outlook). Part A starts with a technical description of the collection of the data, and describes the categories of personal data and data subjects that may be affected by the processing, the privacy options for users and admins, the purposes of the processing, the different roles of the parties, the different interests related to the processing, the locations where the data are stored and the retention periods. In this section, factual contributions and intentions from Zoom are included, as based on public information and their answers to the letter with legal questions.

Part B provides an assessment (by Privacy Company, with input from SURF) of the lawfulness of the data processing. This analysis begins with an analysis of the extent of the applicability of the GDPR and the ePrivacy Directive, in relation to the legal qualification of the role of Zoom as provider of the cloud conferencing services. Subsequently, part B assesses conformity with the key principles of data processing, including transparency, data minimisation, purpose limitation, and the legal ground for the processing, as well as the necessity and proportionality of the processing. Part B also addresses the legitimacy of transfer of personal data to countries outside of the European Economic Area (EEA), as well as Zoom's compliance with the exercise of data subjects' rights.

Part C assesses the risks for data subjects, in particular with regard to the collection of Diagnostic Data and the default settings.

Part D assesses the remaining measures that can been taken by Zoom and the individual universities and government organisations to mitigate the remaining low risks identified in this DPIA, as well as their impact.

This DPIA was conducted between September 2020 and February 2022.

[17] The Model Data Protection Impact Assessment federal Dutch government (PIA). For an explanation and examples (in Dutch) see: https://www.rijksoverheid.nl/documenten/ rapporten/2017/09/29/model-gegevensbeschermingseffectbeoordeling-rijksdienst-pia

Part A. Description of the data processing

This first part of the DPIA provides a description of the characteristics of the personal data that may be generated and processed by Zoom as a result of the use of Zoom Enterprise Meetings.

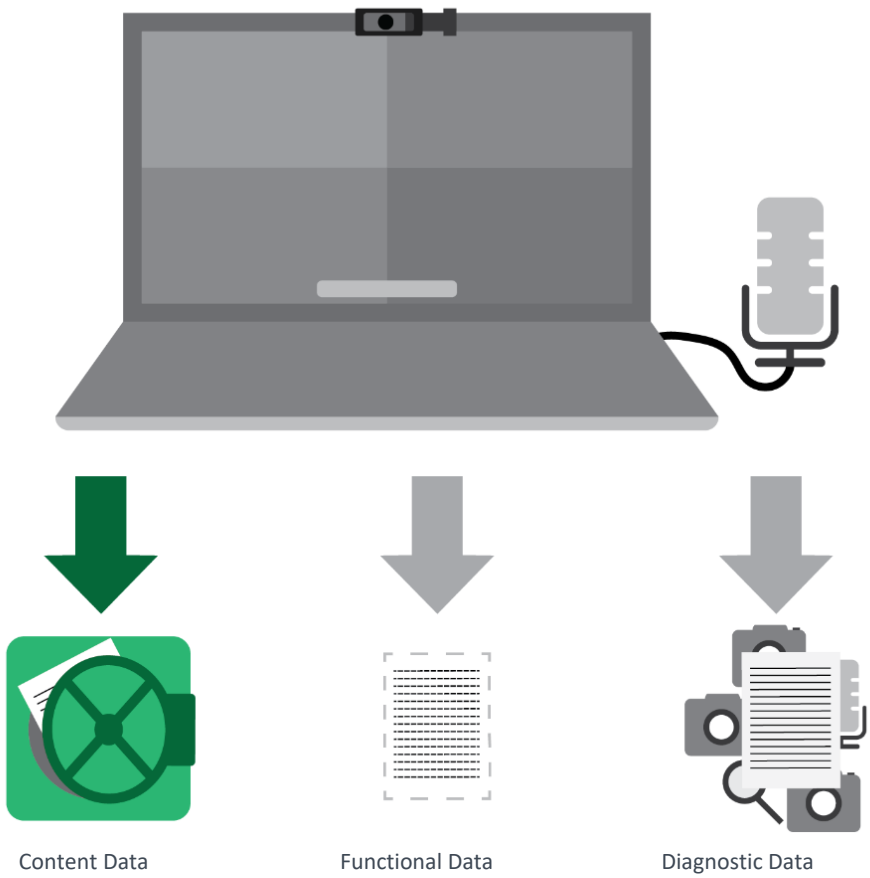
This Part A starts with a short description of the processing of different kinds of data. It continues with a description of the different categories of personal data that may be processed in the Diagnostic Data, the categories of data subjects that may be affected by the processing, the available privacy choices, the purposes of the processing by Zoom, the locations where data may be stored, processed and analysed, and the data protection roles of the universities and government organisations on the one hand, and the role of Zoom as data processor and/or as (joint) data controller on the other hand.

Finally, this part A provides an overview of the different interests related to the processing, of Zoom's treatment of the rights of data subjects, and of the retention periods.

1. The processing of personal data

This Section 1 provides a general overview of the categories of personal data processed by Zoom as a result from the use of the Zoom Meetings Services on the different platforms.

Figure 1: Content Data, Functional Data and Diagnostic Data



This report distinguishes between three main categories of personal data:

Content Data are the video- or chat recordings or transcripts made with Zoom Meetings.

Diagnostic Data include all data generated or collected by Zoom about the use of Zoom Meetings including limited Webinar functionalities, including all possible features, as well as use of the (free and paid) Zoom account. Diagnostic Data include Telemetry Data sent through the applications, as well as website and cookie data.

Functional Data are necessarily processed to execute desired functionalities remotely, on Zoom's cloud servers. Functional Data are out of scope of this report, as long as these data are only data in transit, and not stored by Zoom. Examples of such Functional Data are the technical data about the end-user device necessary to deliver the communication, and the data stream necessary to allow the end user to participate on invitation or to verify if the end user has an authorised Zoom Account.

The key difference between Functional Data and Diagnostic Data as defined in this report, is that Functional Data are and should be transient. This means that these data should be immediately deleted or anonymised upon completion of the transmission of the communication. Otherwise, they qualify as Content Data or as Diagnostic Data.

In its new (February 2022) Privacy Data Sheet, Zoom itself defines 6 categories of personal data: Customer Content, Diagnostic Data, Account Data (end users), Account Holder Data, Support Data, Website, and Feedback and Marketplace Data. For each category, Zoom describes the detailed contents.[18]

1.1. Content Data

Because Zoom Meetings is a cloud service, Zoom processes the audio and video contents of the meetings, the recordings, stored transcripts and chat logs on a combination of cloud-based and colocated data center facilities.

Since the end of January 2021, Zoom offers its EU Enterprise and Education customers a geolocation choice: to have a limited subsection of the Content Data exclusively processed in the EU data (in a datacentre in Germany). Zoom does not offer such a choice (yet) for the Diagnostic, Support, and Account Data of end users, or for the contacts and calendars they actively import in their Zoom services. The transfer of personal data to countries outside of the European Economic Area will be discussed in more detail in Section 8 of this DPIA.

- Customer Meeting and Webinar Communication Content includes:
    - Video, audio, whiteboard, captions, and presentations
    - In-meeting Questions & Answers, polls, and survey information (not possible if E2EE is enabled)
    - Closed captioning (Live Transcription, not possible if E2EE is enabled)

[18] Zoom Privacy Data Sheet, February 2022, URL: https://explore.zoom.us/media/privacy-data-sheet-feb.pdf.

- Chat Messages in 1:1 in-meetings and group chat messages that are not transferred to a permanent chat channel.
- Customer Initiated cloud recordings (Not possible if E2EE is enabled)
- Video recording of video, audio, whiteboard, captions, and presentations (only local recording if E2EE is enabled)
- Audio recording (only local recording if E2EE is enabled)
- Text file of all in meeting group chats (only local recording if E2EE is enabled)
- Audio transcript text file (not possible if E2EE is enabled)

- Meeting and Webinar Participant Information includes:
  - Registered participant name and contact details; and any data requested by Customer to be provided in conjunction with registration
  - Email addresses
  - Status of participant (as Host, as participants in a chat or as attendees)
  - Room Names (if used)
  - User categorizations (labels)
  - Tracking fields such as department or group
  - Scheduled time for a meeting
  - Topic names
- Stored Chat Information is data at rest (in storage) and includes:
  - Chat messages
  - Files exchanged via Chat
  - Images exchanged via Chat
  - Videos exchanged via Chat
  - Chat channel title
  - Whiteboard annotations
- Address book Information. Zoom account administrators can enable end users to integrate their calendar and contacts. Zoom supports Google Calendar, Microsoft Exchange and Microsoft Office 365.[19]
- Calendar Information. This includes meeting schedules made available through Customer controlled integrations (e.g., Outlook, Google).

[19] Idem.

1.2. Diagnostic Data

Zoom collects Diagnostic Data about the individual use of the Zoom Meetings in multiple ways, by collecting Telemetry Data from the mobile and desktop apps and by generating usage and user activity logs on its own cloud servers. When Zoom collects data with cookies and similar technologies about visitors of its website, such data are also Diagnostic Data. However, the category of Website Data is analysed as a separate category of data in this DPIA, to reflect the separate ePrivacy rules for cookies in the Dutch Telecommunications Act.

For this DPIA the contents of the different Diagnostic Data have been verified through interception of the network traffic and inspection of the server logs. The results are described in more detail below, in Sections 2.2 (Legal Definitions Zoom) 3.1 (Audit logs and reports), 3.2 (Telemetry Data), 3.3 (Data Subject Access Requests) and 3.4 (Website Data incl. cookies).

In its Privacy Data Sheet[20], Zoom distinguishes three categories of Diagnostic Data: Meeting Metadata, Telemetry Data, and Other Service Generated Data. Zoom specifies in its Privacy Data Sheet that Diagnostic Data do not include a Zoom user's name, email address, or (other) Content Data, because they are part of the separate category of Content Data. Diagnostic Data also include data in the webserver access logs, but this category of data is described separately below as Website Data.

- Meeting Metadata are metrics about Service usage, including when and how meetings were conducted. This category includes:
    - Event logs (including action taken, event type and subtype, in-app event location, timestamp, client UUID)
    - userID and meeting ID
    - Meeting session Information, including frequency, average and actual duration, quantity, quality, network activity, and network connectivity
    - Number of meetings
    - Number of screen-sharing and non-screen-sharing sessions
    - Number of participants
    - Meeting host Information
    - Host Name
    - Meeting Site URL
    - Meeting start/end time
    - Join Method
- Telemetry Data is information sent to Zoom from the Zoom client software running on an end user's device about how Zoom is used or performing (e.g., product usage and system configuration).

[20] Zoom Privacy Data Sheet, February 2022, URL:https://explore.zoom.us/media/privacy-data-sheet-feb.pdf.

Zoom explains all Telemetry Data follow a similar structure. A few fields describe the client and the operating system, the type- and subtype of the event, the location in the app where the event occurred, a timestamp, and some pseudonymous identifiers, including a UUID, userID and meeting_id. Telemetry Data does not include Content Data, or information about other users, meeting names or other user-supplied values such as profile names. Some fields are common for all events:

- Event time
- Client type
- Event location
- Event
- Subevent
- UUID
- Client version
- UserID
- Client OS
- Meeting ID

Zoom currently describes 42 specific subevents in its Privacy Data Sheet, and has committed to gradually expand this list and keep it up to date. As described in Section 3.2, the technical inspection of the data processing in October and November 2020 showed 49 unique events.

- Other Service Generated Data is other Diagnostic Data collected by Zoom to provide the services requested by the end-user or Customer, such as providing spam warning notices or push notifications. Other Service Generated Data also includes a Zoom persistent unique identifier that Zoom's Trust and Safety Team in the USA combines with other data elements including IP address, data center, PC name, microphone, speaker, camera, domain, hard disc ID, network type, operating system type and version, and client version. Zoom uses these data to identify and block bad actors that threaten the security and integrity of Zoom Services. These data are only accessible by Zoom employees with a need to know and subject to appropriate technical and organisational measures.

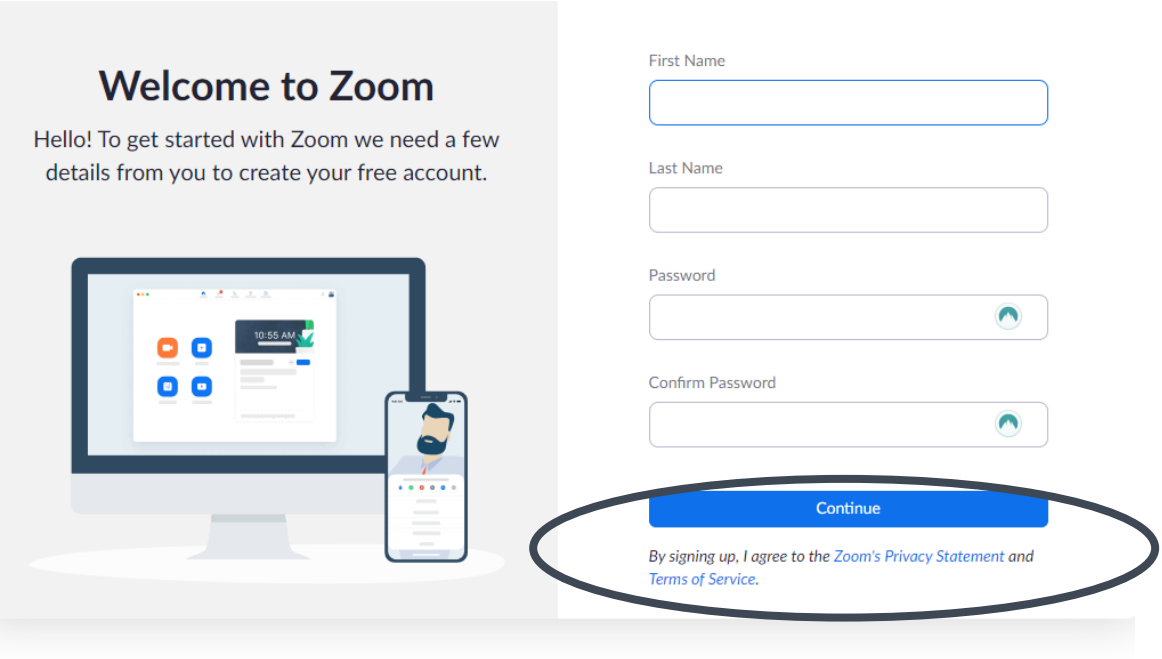
1.3. Account Data (end users and administrators)

To participate in a Zoom Meetings conference call, it is not necessary to create a Zoom account. People can also participate as guest unless the account administrator has configured the account to prevent this.

Zoom explains: "*If someone invites you to their meeting, you can join as a participant without creating an account. However, if the host has restricted joining meetings using authentication profiles, then the participant will need a Zoom account to access the meeting.*"[21]

In practice, employees of the Dutch government and of the Dutch universities will be obliged to use a Zoom Account. Without a Zoom Account they cannot host and schedule meetings, but may also be prevented technically from participating in meetings organised by their own organisation. An organisation with an Enterprise or Edu license may decide through admin settings to only allow participants logged in to a Zoom account. That means the invitee needs to have an e-mail address belonging to one or more specific domains, such as the organisation's domain name.[22]

Figure 2: Registration for a new Zoom account in an Enterprise license[23]



Enterprise and Education end users can sign-up in three ways: (i) with their work or university email address, (ii) through Single Sign On (SSO), or (iii) by using their existing Google or Facebook accounts. When the end user signs up directly (if the organisation does not use SSO), Zoom asks for acceptance of its (consumer) Privacy Statement and Terms of Service. See Figure 2 above. These terms are not valid for Enterprise and Education customers. Besides, forced 'agreement' with a privacy statement can never lead to valid consent. In reply to this DPIA, Zoom confirmed it is not able to change the information on this sign-up screen for EU Enterprise and Education customers.[24]

[21] Zoom, Do you need an account to use Zoom?, URL: https://support.zoom.us/hc/en-us/articles/206175806-Frequently-asked-questions#:~:text=Do%20you%20need%20an%20account,participant%20without%20creating%20an%20account .

[22] Zoom, Authentication Profiles for meetings and webinars, URL: https://support.zoom.us/hc/en-us/articles/360037117472.

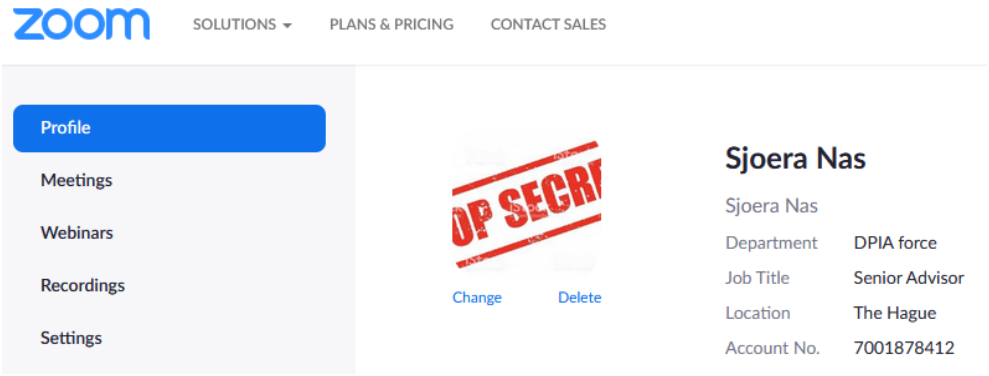
[23] New screenshot made on 16 February 2022.

[24] Zoom e-mail to SURF, 14 February 2022.

Organisations are not obliged to provide the first and last names of each user. They can also prevent providing a directly identifiable email address to Zoom by using SSO. Zoom writes: "*SSO allows the customer to provide a tokenised email address to Zoom to validate that a user is permissioned to use Zoom as part of the customer's account. With this token the customer has to provide a unique identifier for the user and has the option to provide email, surname and given name. In Zoom, the email address is used to provide some service to the user, like sending recording links, and the surname and given name are used to create the display name (used in meetings and in chat to identify the user).*"[25]

End users can choose to actively provide profile data to Zoom, such as a picture, Department, Job Title and Location.[26] For this test, a picture was chosen with the words 'top secret' (See Figure 3 below).

Figure 3 Optional information in Zoom account profile[27]



According to Zoom's Privacy Data Sheet, depending on how the account administrator has configured the Zoom Education or Enterprise account, Account Data include:

- Zoom unique user ID
- Social media login (optional)
- profile picture (optional)
- Display name
- Customer authentication data (unless Single Sign On (SSO) is used)
- Zoom unique ID from guest users that connect to a meeting organised by an EU Education or Enterprise customer

Until the summer of 2021, Zoom also asked for the date of birth when end users signed up for an Enterprise and Edu account. Though Zoom explicitly told users it did not store the date of birth, it was unclear why Zoom (in a role as data processor) collected this information. As a result of the discussions with SURF, Zoom removed this question from the sign-up procedure for its EU Enterprise and Education customers.

[25] Information added based on Zoom's reply to part A of the DPIA, 19 March 2021, p. 16. Zoom also refers to its *Quick start guide for SSO*, URL: https://support.zoom.us/hc/en-us/articles/201363003.

[26] Users can provide this information through the Zoom Account end user interface, URL: https://eu01web.zoom.us/profile.

[27] Name of researcher intentionally included.

1.4. Account Holder Business Data

This is information associated with the individual(s) who are the billing and or sales contact for a Zoom Education or Enterprise account. Zoom only sends unsolicited marketing e-mails to these account holders. Zoom guarantees in the new February 2022 DPA that it does not send marketing e-mails to other account users, such as end users and administrators.

The Account Holder Business Data include:

- Name
- Address
- Phone number
- Email address
- Billing and payment information, and
- Data related to the Customer's account, such as subscription plan and selected controls.

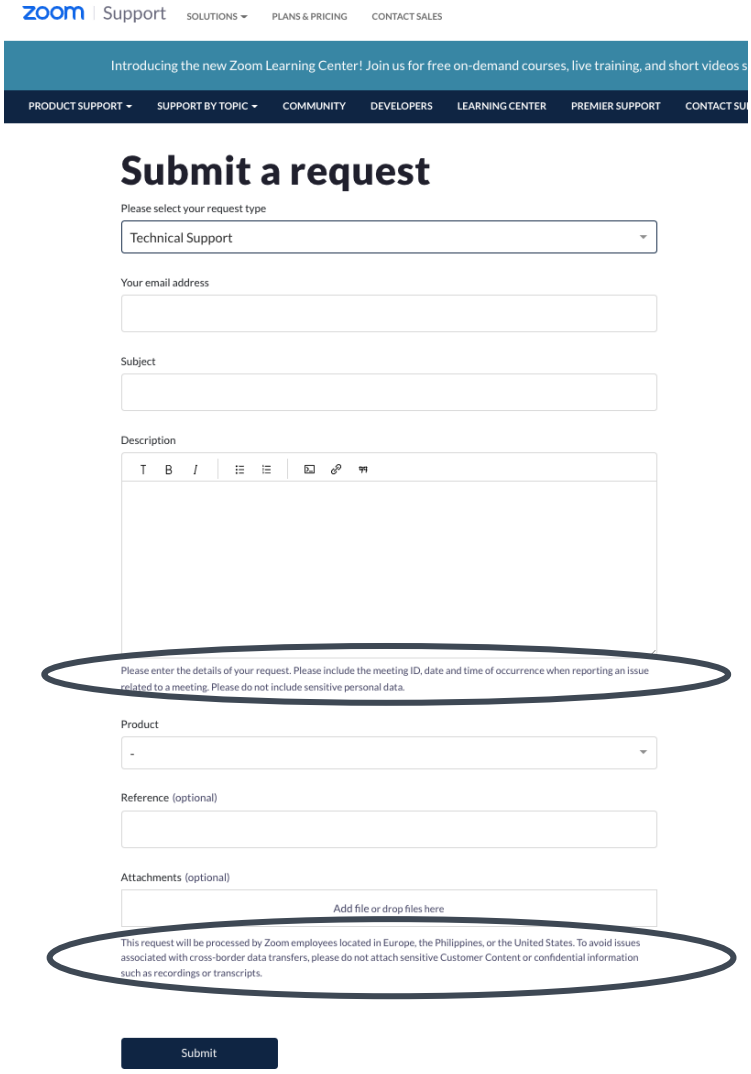
1.5. Support Data

Zoom provides Support Services to its Enterprise and Education customers by providing online resources, including a chatbot, and with chat and phone support through the Zoom Support Center.[28] Zoom uses the US based company Zendesk as a subprocessor to provide its Support Services platform.[29]

[28] Zoom technical support, URL: https://support.zoom.us/hc/en-us/articles/201362003.

[29] Zoom, Third-Party Subprocessors, effective 11 February 2021, URL: https://zoom.us/subprocessors.

Figure 4: Submitting a support request to Zoom



Owners and administrators of Education and Enterprise accounts can file online support requests. The request can include attachments, such as screenshots. Such screenshots may include Content Data. In reply to a request from SURF, Zoom has added two separate warnings to this form, not to upload sensitive data and an explanation that the support requests may be processed in the EU, the USA or the Philippines. See Figure 3 above.

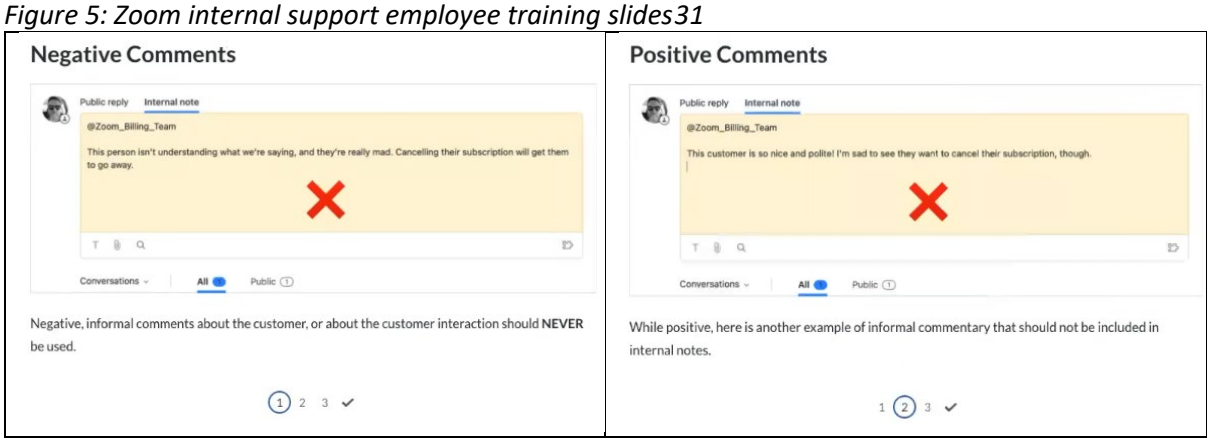
As part of its improvement commitments, Zoom will process Support Data from its EU Enterprise and Education customers in the EU during EU business hours by default, by mid-2022. Once that option is realised, Zoom will add an extra consent question to this form for support outside of EU working hours. Such support can be provided by subprocessors from Zoom in the USA and in the Philippines. Zoom will only transfer the support tickets outside of the EU if the admins explicitly consent to such an incidental transfer of Support Data.

Zoom describes the Support Data in its new Privacy Data Sheet as follows:

"*Support Data is information a customer provides to Zoom or is otherwise processed in connection with support activities such as support bot messages, chats, and phone calls (including recordings of*

those calls) and Service support tickets. The business contacts for a Zoom Education and Enterprise account or the account administrators can submit online support requests. The request can include attachments, such as screenshots. Such screenshots may include (Customer) Content Data or Diagnostic Data."[30]

Figure 5: Zoom internal support employee training slides[31]



Per request of SURF, Zoom created an animated slide deck to train its existing and new support agents not to include any positive or negative comments about the customer in the internal notes about the support request in the support ticketing system. See the screenshots in Figure 5 above.

The actual data processing through a support request has not been tested for this DPIA, in order not to burden Zoom with a fake support request. This DPIA does however assess the risks for data subjects resulting from the use of these services based on the contractual guarantees.

1.6. Website Data

Zoom uses one website, zoom.us, for all online contacts with, and information to, prospective and current users of free and paid accounts. As described in Section 1.1.3 for users of Free and Pro accounts, use of the website is mandatory to log-in to an account.

Zoom acts as a data processor (See Section 6 of this report) for the restricted access webpages, that is, for logged in users and admins. Visitors from the EU are redirected to the EU-hosted Zoom pages when they log in, or when they click on a link to join a meeting.

Zoom is a data controller for its publicly accessible website zoom.us. In both cases, Zoom commits to only set and read strictly necessary cookies by default for visitors from the EU. Zoom has a separate (updated) Cookie Policy.[32] If organisations want to prevent transfer of personal data to Zoom's US-hosted publicly accessible website, they can require employees to use Single Sign On and invite employees to log-in via such a self-defined subdomain, such as 'universityofamsterdam.zoom.us.' Zoom explained in reply to part this DPIA: "*These vanity URL pages are almost entirely customer controlled and would only have cookies on those pages if the customer placed cookies. Zoom does not*

[30] Zoom Privacy Data sheet, February 2022, URL: https://explore.zoom.us/media/privacy-data-sheet.pdf.

[31] Slide deck provided by Zoom on 1 February 2022.

[32] Zoom Cookie Policy, last updated 11 February 2022, URL: https://explore.zoom.us/en/cookie-policy/.

place marketing cookies on such Vanity URLs." [33] Zoom has also confirmed that all traffic such vanity URLs from EU customers stays within the EU datacentres of Zoom (actually, Zoom's subprocessor AWS).

Zoom's Website Data include:

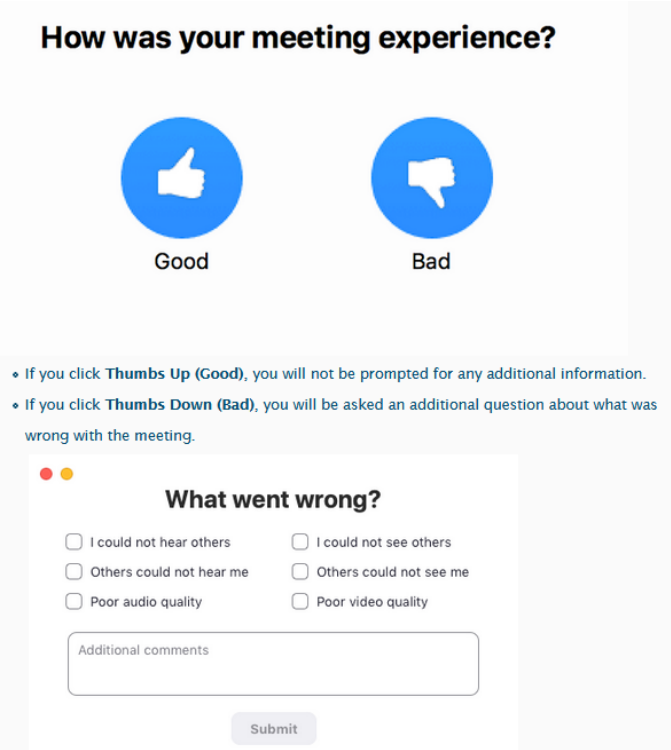
- Strictly necessary cookies as specified in the Cookie Statement
- Internet protocol (IP) address
- Browser type
- Internet service provider (ISP)
- Referrer URL
- Exit pages, the files viewed on our website (e.g., HTML pages, graphics, etc.),
- Operating system
- Date/time stamp
- Approximate location (e.g., nearest city or town, derived from IP address)

1.7. Feedback and Marketplace Data

Zoom can process two additional types of data, but only if the admin enables functionalities. Access to these functionalities is disabled by default for EU Education and Enterprise customers.

[33] Zoom reply to part A of the DPIA, 19 March 2021, p. 16.

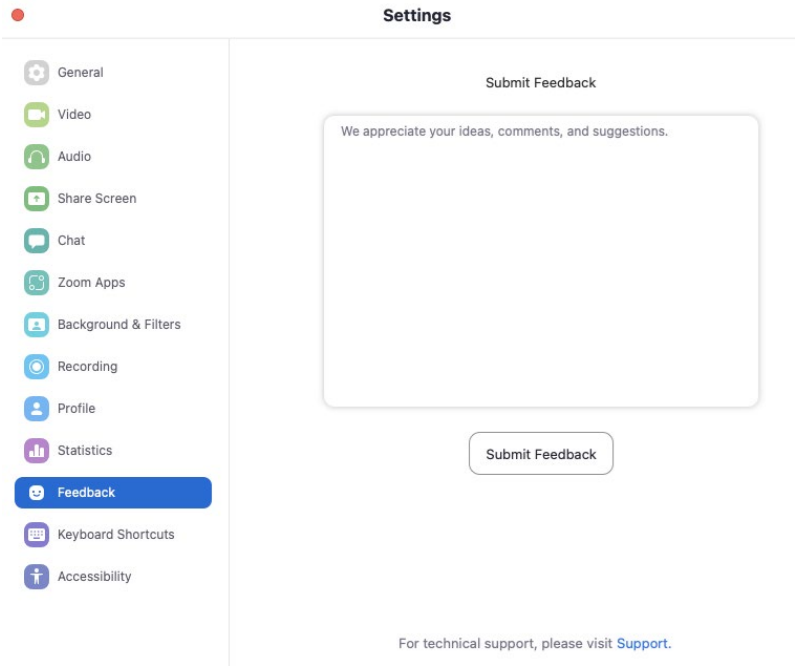
Figure 6: Zoom Feedback question



Feedback is a tool that asks end-users to rate the quality of a conference call at the end of a meeting, by selecting a thumbs up or thumbs down icon. If they are not satisfied, they can answer more questions, and enter free text in an open text field. See Figure 6 above.

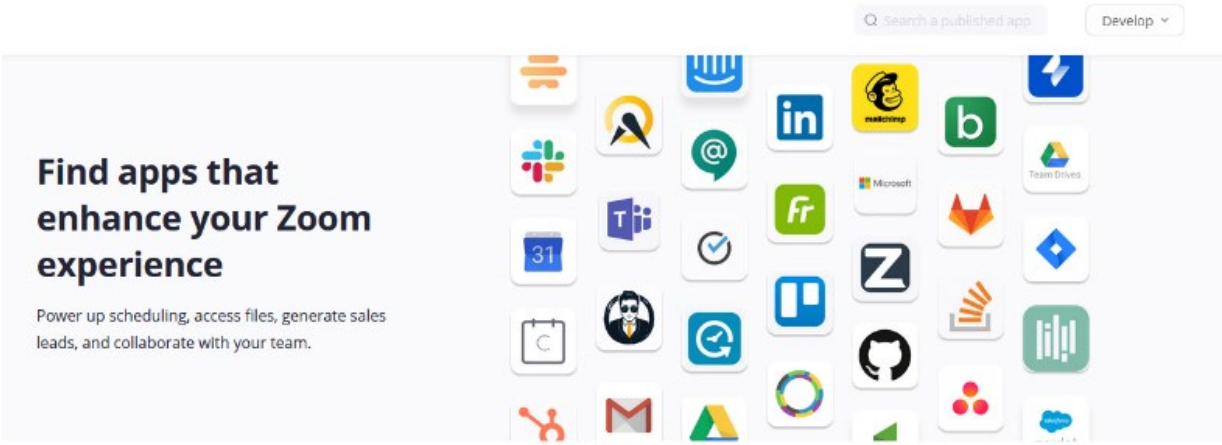
There is a second way for end users to provide Feedback to Zoom, by actively selecting the Feedback option in the Settings menu in their Zoom client (Figure 7 below). Zoom does not actively promote this option, and it cannot be disabled by admins.

Figure 7: Alternative way for end users to provide Feedback to Zoom



Zoom also offers access to third party apps via the App Marketplace (See Figure 8 below). If the administrator allows access to third party apps, and end users installs such an app, they can give access to their Zoom Account via the API. This can be useful, if they want to authorize a chatbot to send messages on their behalf in Zoom. Access to the API is turned off by default (See Section 4 of this report for the available privacy controls and default settings). The user needs to authorise any permissions asked by third party applications.

Figure 8: Zoom App Marketplace



In the new DPA Zoom commits to perform a best effort check on apps to prevent the appearance of malware. However, the third-party apps are independent data controllers for the data processing once integrated. Therefore, this data processing is also out of scope of this DPIA.

2. Legal facts: enrolment framework

The Dutch government DPIA model requires that this Section 2 provides a list of the kinds of personal data that will be processed via the Diagnostic Data, and per category of data subjects, what kind of personal data will be processed by the product or service for which the DPIA is conducted. In this slightly modified version of the DPIA, this question is addressed in two separate sections. This Section 2 provides a description of the legal facts and definitions following from the newly agreed contract with Zoom for the Dutch universities and Dutch government organisations.

Section 3 is focussed on the technical facts about the Diagnostic Data collected by Zoom, including the Telemetry Data from the apps and the Website Data. This Section will also draw conclusions whether the Diagnostic Data are personal data.

Because this is an umbrella DPIA, this report can only provide an indication of the categories of personal data and data subjects that may be involved in the data processing within the Dutch government and the universities. These are outlined in Sections 3.5.1 and 3.5.2 of this report.

2.1. The enrolment framework for Zoom Meetings

Zoom generally offers Zoom Enterprise services for online enrolment, to be procured through its website. However, SURF works with a generic procurement system, through a specific dashboard (DPS, *Dynamic Purchasing System*). This system is not only used by the Dutch universities but also by Irish institutions united in HEAnet. DPS includes a different version of the first three documents of Zoom's enrolment framework.

Zoom's (new) enrolment framework consists of the following documents:

- Order Form determining the number of licenses, services and pricing (*not for SURF/HEAnet),
- Zoom Master Subscription Agreement (Zoom MSA[34]) (*not for SURF/HEAnet),
- Zoom Services Description (Exhibit A of the customised Zoom MSA)[35] (*not for SURF/HEAnet),
- Zoom (new) Data Processing Agreement (The Addendum or Zoom DPA[36]) with appendices,
- New (June 2021) Standard Contractual Clauses for the transfer of data from the EU to the USA, Model 1 and Model 2,[37],

[34] Zoom Master Subscription Agreement. Zoom does not publish its Master Subscription Agreement. Large scale customers such as the Dutch government and SURF may enter into a specific offline Master Subscription agreement. For this DPIA a customized version 5 of the MSA was used provided by Zoom to SURF in July 2021.

[35] Zoom Services Description, effective 8 December 2020, URL: https://zoom.us/docs/en-us/services-description.html. The same content is attached as Exhibit A *Services Description* to the Zoom customized MSA.

[36] Zoom Global Data Processing Addendum, Version of August 2020, URL: https://zoom.us/docs/doc/Zoom_GLOBAL_DPA.pdf.

[37] Zoom new model SCC, based on the Annex to the Commission Implementing Decision on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/6794 June 2021, URL: https://ec.europa.eu/info/system/files/1_en_annexe_acte_autonome_cp_part1_v5_0.pdf.

- Acceptable Use Policy (Community Standards),[38] and
- Zoom Cookie Statement.[39]

Initially, when the first DPIA was performed, Zoom's enrolment framework included many consumer-oriented legal documents, such as the Privacy Statement. As shown in Figure 2 Zoom forced users to accept the applicability of its Privacy Statement and Terms of Service when an end user created a new Zoom account within the Education or Enterprise license. Admins can prevent this by allowing users to sign up via SSO. As explained in Section 1.6, in order to enable SSO they also need to set-up a so-called *Vanity URL*, such as 'universityofAmsterdam.zoom.us'.

In 2021 Zoom's DPA only applied to the limited subset of Content Data, not to any other categories of personal data described in Section 1 of this report. Through Zoom's Terms of Service (included in the MSA), Zoom included other undefined policies published at its website, besides its consumer Privacy Statement.

The negotiated new enrolment framework starts with the improved and expanded (new) Zoom DPA. In the DPA Zoom explains that the provisions in the DPA prevail over all other provisions relating to the processing of personal data: *"In the event of a conflict between the terms and conditions of this Addendum, or the Agreement, an Order Form, or any other documentation, the terms and conditions of this Addendum shall prevail with respect to the subject matter of Processing of Customer Personal Data*."[40] This hierarchy means that nor Zoom nor individual Enterprise and Education customers in the EU can overrule these data protection guarantees by agreeing to other conditions in the order form or the MSA.

2.2. Definitions of different types of personal data

2.2.1. Definitions GDPR

Article 4(1) of the GDPR provides the following definition of personal data: "*'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.*"

The concept of processing is defined in Article 4(2) of the GDPR: "*'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.*"

[38] Zoom Community Standards, URL: https://zoom.us/docs/en-us/community-standards.html.

[39] Zoom Cookie Statement, https://explore.zoom.us/en/cookie-policy.

[40] Zoom DPA, introduction and Clause 14.3: "*If there is any conflict between this Addendum and the Agreement with regard to the subject matter of this Addendum, this Addendum shall prevail to the extent of that conflict.*"

Article 4(5) of the GDPR contains a definition of pseudonymisation: "*the processing of personal data in such a way that the personal data can no longer be linked to a specific data subject without the use of additional data, provided that these additional data are stored separately, and that technical and organisational measures are taken to ensure that the personal data are not linked to an identified or identifiable natural person.*"

The GDPR clearly explains that pseudonymised data are still personal data, to which the GDPR applies. Recital 26 explains: "*Pseudonymised personal data that can be linked to a natural person through the use of additional data should be regarded as data relating to an identifiable natural person. In order to determine whether a natural person is identifiable, account must be taken of all means that can reasonably be expected to be used by the controller or by another person to directly or indirectly identify the natural person, for example selection techniques. In determining whether any means can reasonably be expected to be used to identify the natural person, account shall be taken of all objective factors, such as the cost and time of identification, taking into account available technology at the time of processing and technological developments*."

2.2.2. Definitions Zoom

Zoom uses the following definitions and descriptions of personal data in its (new) DPA:"*Personal Data" means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.*

This includes any special categories of Personal Data defined in Art. 9 of the GDPR, data relating to criminal convictions and offences, or related security measures defined in Art. 10 of the GDPR, and national security numbers defined in Art. 87 of the GDPR and national supplementing law."[41]

In the new DPA Zoom also provides a definition of the term Anonymised Data: "*Anonymised Data" means, having regard to the guidance published by the European Data Protection Board, Personal Data which does not relate to an identified or identifiable natural person or rendered anonymous in such a manner that the data subject is not or no longer identifiable."*[42]

Zoom obtains personal data in different ways, directly and indirectly.

Zoom directly collects personal data from employees and students when they create a Zoom Account and perhaps provide a picture, when they decide to store chat conversations, audio or video recordings (if not technically impossible due to the use of End-to-End-Encryption and permitted under the settings determined by the Zoom account admin), if the account admin enables Feedback submissions or when they decide to actively upload Feedback, or when an admin files a Support Request.

University employees and students enable Zoom to indirectly collect personal data when they visit the Zoom website, schedule a meeting, invite guests or other paid account users to meetings. Zoom can

[41] Zoom DPA, Clause 1.13.

[42] Zoom DPA, Clause 1.2.

indirectly collect personal data about every interaction with its website and cloud Meeting services. Zoom automatically generates such interaction data in system generated logfiles, but has additionally programmed the applications to collect information in telemetry files that are involuntarily sent from portable devices to Zoom. Based on the technical analysis of these data, Section 3 of this report will explain which of these data can legally be qualified as *personal data*.

2.2.3. Legal definitions Content, Account, Support, Website and Diagnostic Data

In its new DPA Zoom uses the umbrella term *Customer Personal Data* to define all the different personal data it processes:

- "*Content Data: All text, sound, video, or image files that are part of profile and End User information and/or exchanged between End Users (including guest users participating in customer-hosted meetings and webinars) and with Zoom via the Services;*
- *(End User and system administrator) Account Data (name, screen name and email address);*
- *Support Data (as described in Annex I to the SCC Appendix);*
- *Website access Data (including cookies);*
- *Diagnostic Data including but not limited to:*
    - *Data from applications (including browsers) installed on End User devices ("Telemetry Data"),*
    - *Service generated server logs (with for example meeting metadata and End User settings) and*
    - *Zoom internal security logs*

  that are generated by, or provided to, Zoom by, or on behalf of, Customer through use of the Services as further defined in Annex I of the Standard Contractual Clauses."[43]

As will be shown in Section 3 below, Zoom's new definition of Customer Personal Data covers all the personal data that Zoom processes in and about the use of Zoom Meeting services.

3. Technical facts: Diagnostic Data

As explained in Section 1.2, Zoom collects Diagnostic Data in multiple ways. This Section summarises the findings of the initial technical analysis performed in October and November 2020, as documented in Appendix 1. In 2021 several new brief inspections were done on the Website Data, lastly on 1 February 2022. The results of these new tests are described in more detail below.

[43] Zoom DPA, Clause 1.9.

In the context of this DPIA four technical inspection methods were used to gain insights in the personal data Zoom generates and processes about the use of its cloud services:

1. Accessing the available reports and log files for admins
2. Interception of outgoing data traffic from the different platforms with Zoom apps
3. Filing of Data Subject Access Requests
4. Interception of Website Data (cookies and similar technologies)

Sections 3.1 to 3.4 summarise the results of the application of each of these methods. All technical findings are shown in detail in Appendix 1 to this report.

3.1. Audit logs and reports

Zoom makes some of its system generated log files available to administrators. Some system generated log files are missing, such as webserver access logs, detailed network security logs and telemetry logs. Zoom does not publish an overview of all the log files it generates and stores on its own cloud servers. However, the existence and contents of some other logs have partially been retrieved by using the other inspection methods discussed below. In response to the initial DPIA, Zoom has committed to gradually increase its transparency about the different Diagnostic Data.

The logs Zoom makes available for administrators are operator logs. Through these audit logs it is possible for administrators (and Privacy Company) to inspect some of the data Zoom collects about the interactions from end-users with its cloud servers. For this DPIA, the logs and reports were compared with the input provided through the scripted test scenarios.

Zoom provides access for admins to the following reports and logs:

- **Zoom daily usage statistics**: show daily number of new users, meetings, participants, and meeting minutes in a month. This report does not contain identifiable data.
- **The active hosts report**: view meetings, participants and meeting minutes within a specified time range. This log file also registers the categorisation given to users. In the test scenarios, three labels were applied and tested: boss, boring and sexy. These labels are visible in the log file, together with directly identifiable data such as Username and User Email.
- **Inactive hosts**: show the users who are not active during a period. This log file shows (identifiable) email addresses and the date of the last login.
- **Upcoming Events**: show at upcoming events each user has. This log file can be queried per host name or host email. This log shows the Start Name and the Topic of the Meeting. In the test scenarios, topic names were used such as ‘Sollicitatiegesprek’ and ‘Inkoopgunning’. These topic names are included in this log. The log includes a directly identifiable first and last name as Host Name, and an e-mail address as Host.
- **Log files about Meetings**: view registration reports and poll reports for meetings. This log file contains the scheduled time for a meeting, the start time, the topic, the (unique) Meeting ID and the number of attendees.

- **Cloud Recording**: View detailed information about cloud storage usage by host. This functionality was not tested for this DPIA, as the functionality was not available in the initial 'free' test account provided by Zoom. The tool was not retested because this functionality is not available if admins follow the key recommendation to enable E2EE for all Meetings.
- **Remote Support**: View in-meeting support sessions during a certain period. As explained in Section 1.5, Privacy Company did not want to burden Zoom by filing a 'fake' Support request to test the log results.
- **User activities Reports**: these reports show information from 3 different audit logs:
    - Operation Logs,
    - Sign-in/Sign-out Logs and
    - User Disclaimer Logs.

When Privacy Company initially performed the test scenarios, it was given a 'free' test account by Zoom. This account did not allow for access to the log files and reports. When the account was later upgraded to an Enterprise account, Zoom was able to show all historical data from the initial tests. Privacy Company deduced from this setting that Zoom does not show the historical user activity reports to the customer, but still collects those data. In other words: the default setting does not mean Zoom does not collect these data.

Zoom confirmed this analysis in its reply to the DPIA, and wrote: "*Zoom justifies this data collection practice by assuming a distinction between Free and Enterprise accounts. By default, Zoom treats Free users as consumers for whom Zoom is the Data Controller in relation to all personal data collected. Zoom describes and provides the legal basis for such personal data processing in its Privacy Statement. Zoom views Enterprise users, by contrast, as data controllers for much of the personal data it collects.*"[44]

Operation Logs

This log file contains admin-like activities, also by regular users, such as a user changing her password, and the self-chosen labels given to users (in this case, for example, 'boss'). These logs also contained the Room Passcode in clear text. In reply to this finding Zoom wrote it expected this to be fixed in April 2021.[45] Privacy Company retested this and confirmed the removal in May 2021.

Sign-in/Sign-out Logs

These user activity logs contain information about the sign-in and sign-out times per identifiable user (user email address), no other user activities. This log also contains the IP address, Client Type (such as 'browser', 'mac', or 'android') and version.

User Disclaimer Logs

This log shows the disclaimer type and status of users within up to a month. Admins can show a disclaimer when users start or join a meeting (desktop client, mobile app, or web client), or sign-in to the web portal. Users must agree to the disclaimer to start or join a meeting, or sign-in to the web

[44] Zoom reply to part A of the DPIA, 19 March 2021, p. 29.

[45] Ibid.

portal.[46] The admin can use this disclaimer to show information about the organisation or show behavioural rules.

- **Chat history**: view archived chat messages in the account. Privacy Company did not change the default setting. As a result, no chat history was logged, though this log does contain the email addresses of the participants to a chat, and the time when the last message was sent.
- **Schedule tracking fields**: View or edit fields that can be used to analyse Meetings usage. By default, no such specific fields are provided. As part of the test scenarios, Privacy Company used the fields 'Team', 'HR' and 'Klantcontact'. These names return in this log.

Initially, Zoom did not publish much information about the different personal data it processed in these logs. Zoom's first mitigation proposal omitted to mention different categories of personal data observed in the logs. However, all of these missing data are now included in the description of Content Data in the new Privacy Data Sheet, under *Meeting and Webinar Participant Information*.[47]

3.2. Telemetry Data

Zoom does not offer any tools similar to the Data Viewing Tool provided by Microsoft for end-users to see what Telemetry Data have been sent from their apps. Nor does Zoom provide access via tools for admins to see the Telemetry Data that are automatically sent to Zoom from the end-user devices.

Initially, interception of the traffic generated by the iOS and Android apps was not possible with the regular MiTM procedure, because the traffic was protected against interception with certificate pinning. Instead, the traffic was intercepted with Wireshark. This resulted in a higher level of uncertainty about the contents of the captured network traffic from the apps.

In November 2020 Zoom informed Privacy Company about workarounds to intercept the Telemetry Data from the iOS and Android apps. Based on that information, a second test run was conducted on the apps on both operating systems. Privacy Company was then able to (separately) capture and analyse the telemetry traffic.

Zooms sends log events to its own servers as a POST request. Below are two examples of two such POST requests.

The first example (from MacOS) contains two events, sent to the URL:
https://eu01logfiles.Zoom.us/stat/append/3bdDCvtUdtgM7X%2BuLZf79WlDIu7jTmLQ2YNzdDLgl7A%3D:

[46] Zoom, Creating a custom disclaimer, URL: https://support.zoom.us/hc/en-us/articles/360051221831#h_01EN986NNCPQR7RW9Y8WVQNEN1.

[47] Zoom Privacy Data Sheet, February 2022, URL:https://explore.zoom.us/media/privacy-data-sheet-feb.pdf.

Figure 9: Example of Telemetry event from Zoom on MacOS


```
{
 "client_os":"mac",
 "client_type":"Zoom Main Client",
 "client_version":"5.3.52877.0927",
 "event":"Tap Security",
 "event_loc":"In Meeting",
 "event_time":"9/30/2020 12:19:40",
 "in_sharing":"0",
 "meeting_id":"focAptkITTSfHTiULJWSIw:=",
 "sub_event":"",
 "user_id":"6n1pCAW4TT2qj5tmnGoKSg",
 "uuid":"3bdDCvtUdtgM7X uLZf79WlDIu7jTmLQ2YNzdDLgl7A="
}
{
 "client_os":"mac",
 "client_type":"Zoom Main Client",
 "client_version":"5.3.52877.0927",
 "event":"Recording",
 "event_loc":"In Meeting",
 "event_time":"9/30/2020 12:20:51",
 "meeting_id":"68460188777",
 "record":"toolbar-button",
 "sub_event":"Cancel",
 "user_id":"6n1pCAW4TT2qj5tmnGoKSg",
 "uuid":"3bdDCvtUdtgM7X uLZf79WlDIu7jTmLQ2YNzdDLgl7A="
} ….
```


Figure 10: Another telemetry example from Zoom on Windows:


```
{
        "client_os":"win7",
        "client_type":"Zoom Main Client",
        "client_version":"5.3.52879.0927",
        "event":"Adjust Settings",
        "event_loc":"In Meeting",
        "event_time":"9/30/2020 12:27:14",
        "sub_event":"UnMute",
        "uuid":"MWPXi9JgWviIbBVGzwqm6Y v FOuzuOmLUPKd72ggBM:"
}
```


All observed Zoom-telemetry follow a similar structure: a few fields describe the client and the operating system, the type- and subtype of the event, the location in the app where the event occurred, a timestamp and some unique identifiers, including a UUID, userID and meeting_id.

Privacy Company did not observe any Content Data in the intercepted telemetry events. The events also did not contain information about other users, meeting names or other user-supplied values such as profile names.

Zoom has used these observations to improve its public documentation, and confirms these findings in its new (February 2022) Privacy Data Sheet.

Telemetry Chrome plugin

The activity of scheduling a meeting displays a form where meeting details can be entered. No network traffic from the plugin was observed while filling in the form. Only when a user clicks on the "Save and Continue" button, a single POST request is made to https://eu01web.Zoom.us/ mimo/save_setting with the meeting details.

Telemetry Outlook plugin

The Outlook plugin does not send any Telemetry Data to Zoom, only functional traffic, such as loading the profile image and the login to the service.

In total Zoom collects 49 different telemetry events. In the technical test, in total 240 telemetry events were observed in the outgoing network traffic from the 5 tested platforms and 2 plug-ins. Zoom explained that in total, over all platforms, Zoom could have collected 277 telemetry events. The 49 unique telemetry events are a very low number, compared to other telemetry streams collected by cloud providers (as inspected by Privacy Company for other DPIA reports). The contents of these telemetry events are unsurprising, with the exception of the UUID and UID.

Initially, Zoom stated it only needed to process aggregated Telemetry Data to evaluate the functionality of the app, not any individual user actions. With that purpose, there was no obvious justification to include the two pseudonyms UUID and User ID in the telemetry events. However, in reply to the initial DPIA, Zoom explained why telemetry events are also needed on an individual (pseudonymised) level, for the purposes of abuse and fraud prevention, and for technical troubleshooting upon Customer request.

Based on the technical analysis and the (newly updated) public information, the telemetry events appear to contain adequate, and not excessive, personal data for the agreed purposes of Zoom (in a role as data processor).

3.3. Data Subject Access Requests (DSARs)

Zoom explains in the new DPA that it is primarily the customer's responsibility to answer Data Subject Access Requests (DSARs), but that Zoom will assist its customers to help answer the requests. Zoom also commits to build two self-service tools: one for the admins to easily produce an overview of all Diagnostic Data relating to a specific user, and a do-it-yourself tool for end users. These tools will be ready before the end of 2022. Prior to that, Zoom has committed to ensure that it will manually provide all requested data.

Zoom writes in the DPA:

"*To the extent that Zoom is a Processor:*

8.1 Zoom shall promptly notify Customer upon receipt of a request by a Data Subject to exercise Data Subject rights under Applicable Data Protection Law. Zoom will advise the Data Subject to submit his or her request to Customer, and Customer will be responsible for responding to such request.

8.2 Zoom shall, taking into account the nature of the Processing, assist the Customer by appropriate technical and organizational measures, as far as this is possible, for the fulfilment of the Customer's obligation to respond to requests for exercising the Data Subject's rights (regarding information, access, rectification and erasure, restriction of Processing, notification, data portability, objection and automated decision-making) under Applicable Data Protection Law. Zoom commits to develop two types of automated Data Subject Access Request tools listed in order of priority: an export tool of individual personal data for Account administrators and a do-it-yourself take-out tool for individual end-users."[48]

Two DSARs were sent to Zoom on 12 October 2020 for the two test accounts. The requests were filed in order to be able to compare the data collected from the outgoing traffic with the data that Zoom knowingly collects. Initially, Zoom referred by e-mail of the same day to the information available in-product for users and in the console for Zoom administrators.[49] On 13 November 2020 Zoom constructively replied with a more substantial response to the access requests. The response contained the following information (see Appendix 1):

- Additional (opaque) identifiers attached to both test-accounts. The identifiers appear to be base64-encoded values with no explained or discernible structure.
- An explanation that data that is connected only to an IP address, not to other identifiers, cannot be used to uniquely identify an individual.
- A short description of Meeting Logs. This log was included in the response. The log contained several unique user and/or machine identifiers.
- A short description of Event Logs (called Telemetry Data in this DPIA). This log was included in the response, and contained 277 events. The logs contain several unique user and/or machine identifiers.
- A short description of Account Logs. This log was included in the response. The log contains several unique user and/or machine identifiers.
- Web request logs. No details provided about the cookies and traffic sent to third parties. Zoom explained with the following statement why it did not provide third party data:

  "Third-Party Data Not Provided: We have confirmed with the third-parties outlined above that either no data was collected related to any identifiers for the subjects, or that this data was

[48] Zoom new DPA.

[49] E-mail Zoom 12 October 2020. Zoom wrote: "*The administrator of your account as the controller of your data is responsible for providing you with information requested through a valid data subject access request. Please contact your Zoom account administrator to complete your request.*"

not available in an identifiable fashion. Thus, we cannot provide any information pursuant to your request for these third-parties."[50]

- A listing of cookies or other comparable methods used on the Zoom platform, (for logged-in users) by Zoom
- A listing of cookies or other comparable methods used on the Zoom platform (for logged-in users) by a third party
- A listing of cookies or other comparable methods used on the publicly accessible Zoom website by Zoom
- A listing of cookies or other comparable methods used on the publicly accessible Zoom website by a third party

In dialogue about these results of the access requests, Privacy Company explained that Zoom, when it considered itself to be an independent data controller, should respond itself to data subject access requests. If Zoom on the other hand wanted to act as data processor, it should provide the data controller (i.e., the admins of the organisations) with all the information necessary to comply with data subject access requests.

Initially, Zoom qualified itself as a data controller for all data except for the Content Data. At the time, Zoom did not provide sufficient information about the Website Data. With regard to other categories of personal data, Zoom failed to mention the specific purposes of processing for each of the categories, the envisioned retention period of the data; whether or not Zoom applied automated decision making or profiling and what safeguards Zoom had in place for transfers to third countries. This meant that Zoom as controller did not provide its customers with sufficient information to adequately respond to data subject access requests.

As mentioned at the start of this paragraph, Zoom has since committed to become a data processor (factually and contractually) for all personal data, except for the public Website Data, and to help admins provide complete responses to DSARs. Additionally, Zoom has committed to develop a take-out tool for the behaviour of admins, to allow its customers to verify that the logs are not used as an employee monitoring tool.

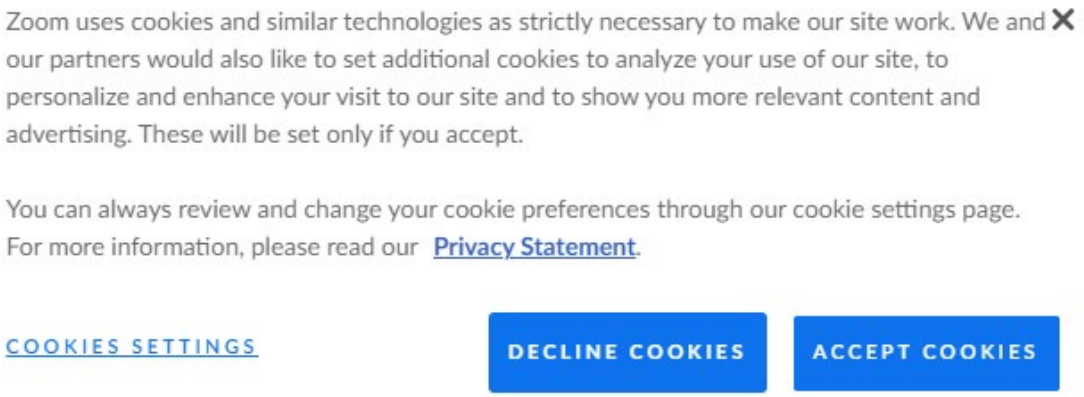
3.4. Website Data (cookies and similar technologies)

Zoom only uses the Zoom.us domain, both for publicly accessible information, and for information that is only available for logged-in users and administrators.

Zoom has replaced its consent management tool, and now uses a tool from the US based company OneTrust to provide choices to website visitors. This tool creates a pop-up for visitors with a consent request (both on the public website and on the restricted access pages). See Figure 8 below.

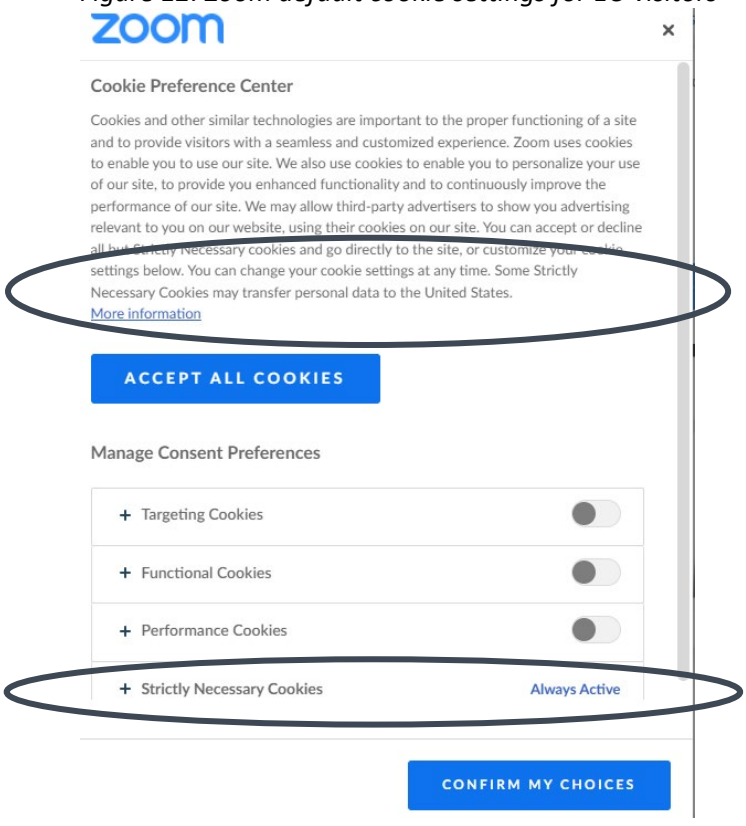
[50] Zoom response to DSAR, 13 November 2020.

Figure 11: Zoom Cookie Consent Manager[51]



As a result of the discussions with SURF, Zoom has changed the default settings for visitors from the EU to its website (both the publicly accessible and restricted access pages), to only set and read strictly necessary cookies. See Figure 12 below. Zoom has contractually committed to continue to monitor and apply this policy in the future. Zoom recognises the origin of its Website visitors based on their IP addresses.

Figure 12: Zoom default cookie settings for EU visitors[52]



Zoom's new default setting for cookies is a major improvement compared to the traffic observed in October and November 2020. At the time, Zoom incorrectly categorized the DoubleClick and Google

[51] Screenshot 2 February 2022.

[52] Screenshot 2 February 2022.

NID advertising cookies as 'Required Cookies' (the lowest cookie level a user could choose). This meant that a user could not prevent these cookies from being set and read.

In reply to this finding Zoom explained it was a mistake in the cookie consent tool. Privacy Company retested the effects of the cookie consent manager on 1 April 2021. It still included a non-specified Google NID cookie as 'required'. According to Zoom's reply, this only referred to the Google ReCAPTCHA cookie technology. However, according to Google's own explanations about its NID cookies, NID is (also) used to show Google ads in Google services for signed-out users. See Appendix 1 for these historical details.

Previously, by allowing its website to set and read tracking cookies without consent, Zoom allowed third parties to collect unique identifiers about the user, in combination with information about the device and the interest in Zoom. If the third party were an advertising network, the identifiers could be shared in an online auction with connected platforms that could in turn, share these data with unknown quantities of other third parties.

In December 2021 and January 2022 Privacy Company retested the Website traffic and information in Zoom's new cookie consent banner. Four third parties were found that set cookies at the strictly necessary level, for which consent was required (segments.company-target.com, match.prod.bidr.io, youtube.com and widget-mediator.zopic.com). On 9 January 2022, those cookies were removed, but there was still traffic to wootric.com (for surveys that should not be conducted at the strictly necessary level) and to Intuition Machines for a hCAPTCHA cookie. In a final retest on 18 February 2022, no more traffic to Wootric was observed at the strictly necessary level, and Zoom committed to remove a final remaining Google reCAPTCA cookie from the webpage where end users can file an appeal against account termination.

Zoom committed to SURF to ensure no traffic is sent to third parties that are not subprocessors at the privacy-friendly default level. Zoom explicitly confirms in its new Cookie Statement: "*For strictly necessary cookies Zoom engages parties that have signed a processor agreement with Zoom in which any processing beyond or outside of Zoom's instruction is explicitly prohibited, including by the third parties' subprocessors.*"[53]

In its (new) Cookie Statement Zoom explains the purposes for the four different categories of cookies. The Statement refers to the detailed lists in the Cookie Consent tool shown in Figure 12 above. Per cookie, the tool informs about name of the cookie, host (domain), retention period (Duration), Type (first or third party), Category, and a description of the purpose.

When end users sign in, Zoom technically redirects its European visitors to its EU-hosted restricted access pages. However, Zoom's public website is hosted in the USA. This means visitor IP addresses would be transferred to the USA when end users and admins visit the public website to look-up help information, or to log-in to their Zoom account if they want to use Zoom via their browser. Zoom has explained that Education and Enterprise customers can prevent this data traffic if they require employees to use Single Sign On via a Vanity URL, such as 'universityofamsterdam.zoom.us'. As quoted in Section 1.6 Zoom explained that it doesn't set any cookies on such URLs.

[53] Zoom Cookie Statement URL https://explore.zoom.us/en/cookie-policy/.

Additionally, to ensure that website visitors are aware of the incidental transfer of personal data (IP addresses with temporary identifiers) to subprocessors in the USA with the strictly necessary cookies, Zoom has added a sentence to its cookie pop-up to make visitors aware of this necessary transfer of personal data to the USA.

In sum, **sections 3.1 to 3.4 show that the Diagnostic Data, Telemetry Data, and Website Data are personal data**. The analysis of the operator logs that are available for administrators shows they contain usernames, email addresses, times, performed activities and qualifiers. The telemetry logs contain User ID's and UUIDS, in combination with device information, information about activities performed in the app with time stamps. These data are generated by (and protected by access credentials) the activities of individual identifiable end users (data subjects).

3.5. Types of personal data and data subjects

As emphasized above, as umbrella DPIA, this report cannot enumerate all possible categories of personal data that can be processed by Zoom and its Education and Enterprise customers in the context of Zoom Meetings. However, this report aims to help the universities and government organisations identify these categories, to help them decide about the actual installation and settings based on an inventory of the categories of personal data that are factually processed in their specific organisation. This DPIA does not assess if organisations can legitimately process these different categories of personal data: this DPIA only examines the risks of the specific use of Zoom to exchange such personal data with individuals in and outside of the organisation, and share some of these personal data with Zoom.

3.5.1. Categories of personal data

Generally speaking, end users can process all kinds of personal data through Zoom Meetings, either in a streaming audio and/or video conference, but also with text in the chat or by sharing images and files through Zoom, and in (local) recordings of the Meetings. If E2EE is not enabled, it is possible to store personal data in cloud recordings and cloud transcriptions of Meetings.

Communication content

The contents of the communications are sensitive, in view of the fundamental right to communications secrecy. Zoom's Meeting services can be used to discuss many different topics by many different organisations. This may for example include location data, salary information, company or personal confidential information), data relating to children under 16 years, and special categories of data. Exchanged, recorded or transcribed conversations may also include personal data relating to criminal convictions and offences or related security measures (Art. 10 GDPR). Additionally, Account Data may be considered confidential, if an employee works for a government organisation with a high level of sensitivity, or sensitive if it concerns a minor.

The names of Zoom Rooms and meetings appear in the log files, as well as labels given to users, such as 'boss'. It is therefore prudent for universities and government organisations to assume that the Zoom Meetings Diagnostic Data can include all categories of personal data, unless the organisations draft and enforce a policy to discourage users from using sensitive personal data for meeting topics and prevent the use of revealing labels to categorise (groups of) users.

Classified Information

Depending on the capacity in which Dutch university or government employees work, they may process confidential government information or state secrets (Classified Information). The Dutch government defines four classes of Classified Information, ranging from confidential within a department (DEP-V) to top secret.[54]

If data contain personal data, according to the Dutch governmental security standard BIO, security measures described for level BBN2 are mandatory. If an organisation applies BBN2, they can process the first level of classified information (DEP-V). According to national policy outlines with regard to the use of cloud services by Dutch government organisations, from a security point of view, data protected at BBN2 level may be stored in a public cloud, subject to additional conditions. However, the BIO security risk categories do not match with GDPR assessments of the data protection risks for data subjects.

Classified Information is not a separate category of data in the GDPR or other legislation concerning personal data. However, information processed by the government or universities that is qualified as Classified Information, regardless of whether it qualifies as personal data, must be protected by special safeguards. The processing of this information may also have a privacy impact if such information relates to a specific individual. If the personal data of a government employee, such as his email address at the domain of his employer, or a unique device identifier, reveals that this person works with Classified Information, the impact on the private life of this employee may be higher than if that employee would only process 'regular' personal data. Unauthorised use of Classified Information could for example lead to a higher risk of being targeted for social engineering, spear phishing and/or blackmailing.

If universities or government organisations do not apply E2EE, they are capable of using Zoom's cloud storage to store audio and video recordings and transcriptions, as well as the chat history. In that case they have to be aware that the information stored on Zoom's cloud servers may include Classified Information from and about employees, including information which employees regularly discuss or share confidential data (for example in the Room Names).

Personal data of a sensitive nature

Some personal data have to be processed with extra care, due to their sensitive nature. Examples of such sensitive data are financial data, traffic and location data. Not only the contents of communication are sensitive, but the metadata (Diagnostic Data) as well, about who communicates with whom. This will be assessed in more detail in Section 17.1.1 of this report.

The sensitivity is related to the level of risk for the data subjects if the confidentiality of such data is breached. The effect of a breach of personal data of a sensitive nature may pose a greater risk for the data subject of being targeted by criminals (e.g., blackmail, identity theft, financial fraud). Government and university employees may also experience a *chilling effect* as a result of the possible monitoring of their behavioural data. The audit logs could for example be used by the employer to reconstruct a pattern of the frequency and length of time spent in Zoom calls, with what other people. This is not

[54] Amongst others, the categories of classified information are defined in the Voorschrift Informatiebeveiliging Rijksdienst – Bijzondere Informatie (VIR-BI).

easy. Zoom does not offer analytic tools for employers to easily create graphs and compare and assess work patterns of groups of employees. Zoom has even decided to remove a privacy invasive analytics tool to analyse attendee attention.[55] However, Zoom has committed to develop a tool to make it much easier for admins to take out all data relating to a specific user, in order to be able to answer Data Subject Access Request. Such a file could be used abusively, for a performance assessment, if use for such purposes is not specifically excluded in an (internal) privacy policy for the processing of employee personal data.

It is likely that many government and university employees will process personal data of a sensitive nature by using Zoom Meetings. For example, teachers can organise oral exams, or interview data subjects about for example health data for surveys. Government employees can use Zoom to discuss sensitive financial data in relation to subsidies. Colleagues can use the chat and file share functionality to send each other detailed questions and answers from and about external individuals. If the use of E2EE is not mandatory, such personal data of a sensitive nature can be stored on Zoom's cloud servers, also as transcripts of conversations.

Zoom added in reply to this DPIA: "*To offset these risks, admins have a range of settings available to them, including to disable recordings entirely or to disable the download feature for recordings.*"[56] These privacy settings are discussed in Section 4 of this DPIA.

Special categories of personal data

Special categories of personal data are strongly protected by the GDPR. According to Article 9 (1) GDPR, special categories of data consist of any:

"*personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation*".

With special categories of data, the principle is one of prohibition: these data may in principle *not* be processed. However, the GDPR contains specific exceptions to this rule. Special categories of personal data may be processed for instance when the data subject has explicitly consented to the processing, or when data are made public by the data subject, or when processing is necessary for the data subject to exercise legal claims.[57]

Employees can (voluntarily) upload a profile picture of themselves. Such a picture *may* reveal ethnicity, religious beliefs or even health data (depending on the context in which the pictures are processed). Employees may also discuss special categories of data. If they store transcripts of such conversations, or chat logs, in Zoom's cloud storage, they enable Zoom to process special categories of data (as a data processor).

---

[55] Zoom, Attendee attention tracking, last updated 15 December 2021, URL: https://support.zoom.us/hc/en-us/articles/115000538083-Attendee-attention-tracking.

[56] Zoom reply to part A of the DPIA, 19 March 2021, p. 42. Zoom refers to its support article on cloud recording, URL: https://support.zoom.us/hc/en-us/articles/203741855-Cloud-recording.

[57] These specific exceptions lifting the ban on the processing are listed in Article 9(2) under a, e, and f of the GDPR.

Similarly, employees can exchange files with special categories of data. If government organisations such as the police and the judiciary worked with Zoom Meetings, they could exchange files with data about crimes or convictions. Similarly, university employees can conduct surveys in prisons about the education of convicts as a prediction for criminal behaviour. If employees use special categories of data as room or meeting names, or qualify guest attendees with categorisations about their health (for example: blind, audio only), such qualifications can become part of the Diagnostic Data (for which Zoom acts as a data processor).

3.5.2. Categories of data subjects

Generally speaking, the different categories of data subjects that may be affected by the processing of personal data through Zoom Meetings can be distinguished in three groups, namely: (i) employees, (ii) registered Education or Enterprise users from other organisations, and (iii) miscellaneous other data subjects (without an Education or Enterprise account).

Employees and students

The university and government end users of Zoom Meeting services are employees, civil servants, contractors, students and (temporary) workers. Their names and email addresses are processed in the Zoom accounts, and are part of some of the operator logs. Their pseudonymous UUID and UID (which can be linked by Zoom and by the organisation admins to their names) end up in the Telemetry Data collected by Zoom, together with basic information about activities performed in the app. Apart from the information created as profile information, and provided to Zoom as hosts of meetings, employees' personal data can also appear in information generated by others. For instance, when they are invited to a meeting organised by a colleague.

Registered other Enterprise or Education users

Zoom facilitates the sharing of information with internal and external contacts. Both the Content Data and the Diagnostic Data may contain information about contact persons that are not employees of the relevant government organisation or university. Examples are employees of other universities or government organisations. If they communicate with each other, their personal data all fall under the same (negotiated) privacy guarantees. These Diagnostic Data may include the participants name and email addresses, as well as the time when the meeting was scheduled and how long it lasted.

Dutch citizens and other data subjects (guest users)

Besides employees and other Education/Enterprise licensed account users, the processing of personal data via Zoom also involves other data subjects, with or without a Zoom account. If a government organisation for example organises video consulting hours with Zoom, citizens can be invited as 'guest' in the licensed organisation environment, or they can use their own free (consumer) account to participate. Similarly, a university may allow students to participate to online classes as guests, or with their free (consumer) Zoom account. Through contacts with other data subjects, Diagnostic Data could include privileged information about the communications pattern with people with professional secrecy such as lawyers. Other examples of external data subjects are future students participating in online introductory meetings, or job applicants. In reply to a question about the applicable data protection assurances when a 'guest' participates with a free consumer account in a Meeting initiated by a Host within an Enterprise or Edu license, Zoom guarantees in the new DPA that their personal

data are protected under the negotiated data protection guarantees for the Dutch universities and government organisations.

In sum, there are no limits to the categories of data subjects whose data may be processed in Customer Data and Diagnostic Data under normal use conditions by employees of the Dutch government and the universities.

4. Data processing controls

This Section 4 discusses the available privacy controls for end-users and administrators to influence the processing of Diagnostic Data, and the processing of personal data through other parties, including external apps. This section also describes the *default* settings of such controls, and situations where admins do not have central privacy controls.

4.1. Privacy controls for end users

This Section describes the 4 different sets of options for end users to minimise the data processing by Zoom. These options are:

1. limiting push messages in the Zoom app on the mobile phone
2. limiting the processing purposes when creating a Zoom account
3. limiting the exchange of personal data when they host a Meeting
4. limiting visibility of their personal data to other participants when they participate in a Meeting

Some of these privacy choices depend on settings determined by the administrator. The options for administrators are discussed in Section 4.2.

4.1.1. Installing Zoom app on a mobile device (iOS and Android)

When a user creates an account on a mobile device, Zoom requests permission to access the following data from (the sensors on) the device:

- Calendar
- Camera
- Contacts
- Precise location
- Microphone
- Telephone
- Storage
- Other (such as prevent phone from sleeping, change audio settings, use fingerprint hardware).

Figure 13: Permissions required in the Android Meetings app[58]

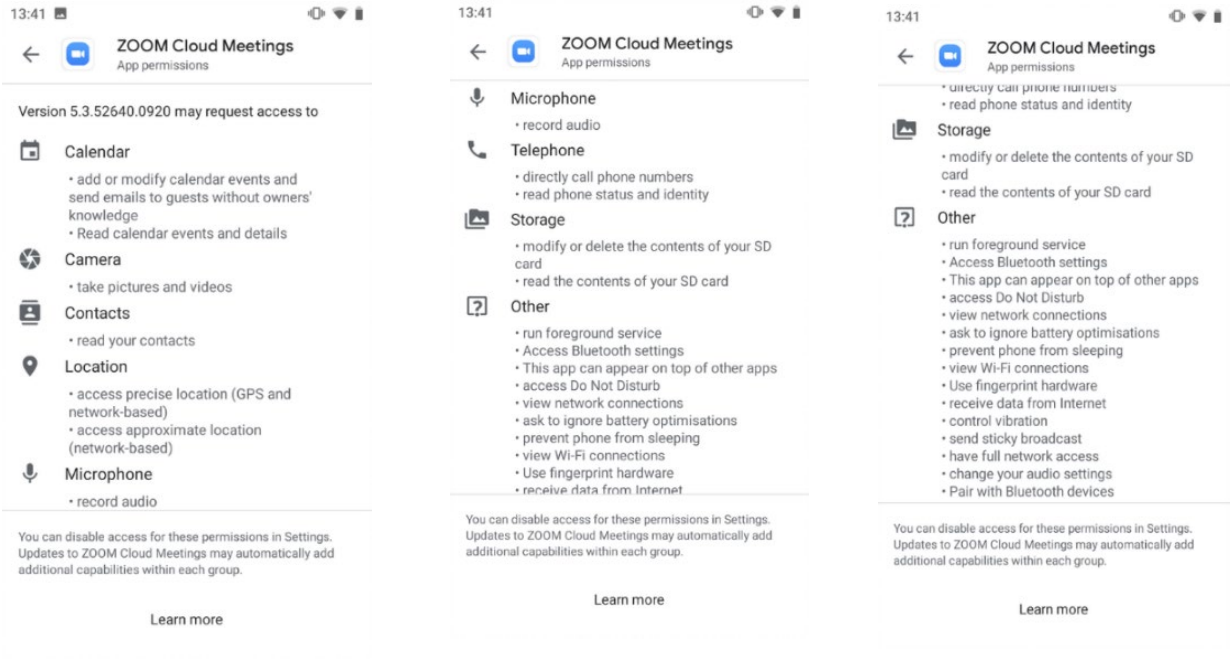
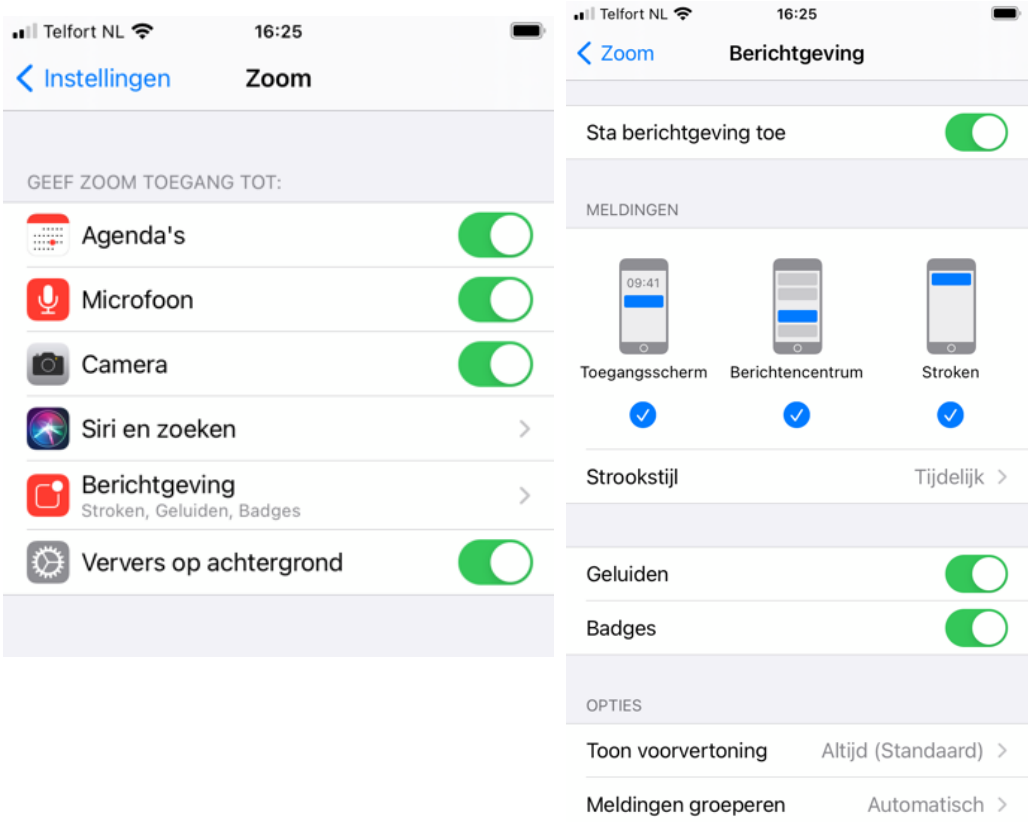


Figure 14: Permissions required in the iOS Meetings app



[58] As recorded on 28 September 2020, in Android app version 5.3.52640.0920, last updated 21 September 2020.

4.1.2. Privacy choices and default settings in Zoom user account

When a user creates a Zoom account, Zoom presents the users with security and privacy choices.[59] In this Section only some privacy options are listed. They have the following default settings:

- Enable E2EE in Account Settings – Meeting- Security (default Off)[60]
- Mirror my video (default on)
- Apply video filters
- Use virtual backgrounds (there is no default background)
- Share Screen (a user can turn this on, if the admin and host have permitted this),
- Edit profile picture (there is no default picture)
- Integrate Zoom with Outlook (default Off)
- Touch up my appearance (default Off)
- Enable the remote control of all applications (default Off)
- Show message preview (default On. Zoom explains: "*uncheck this option for privacy*")
- Record video during screen sharing (default On, if E2EE is not enabled)

In reply to the initial DPIA, Zoom disabled by default the option to submit Feedback with a thumbs up or thumbs down symbol at the end of a meeting for its EU Enterprise and Education customers. This was default On for end-users but default Off for the entire organisation.

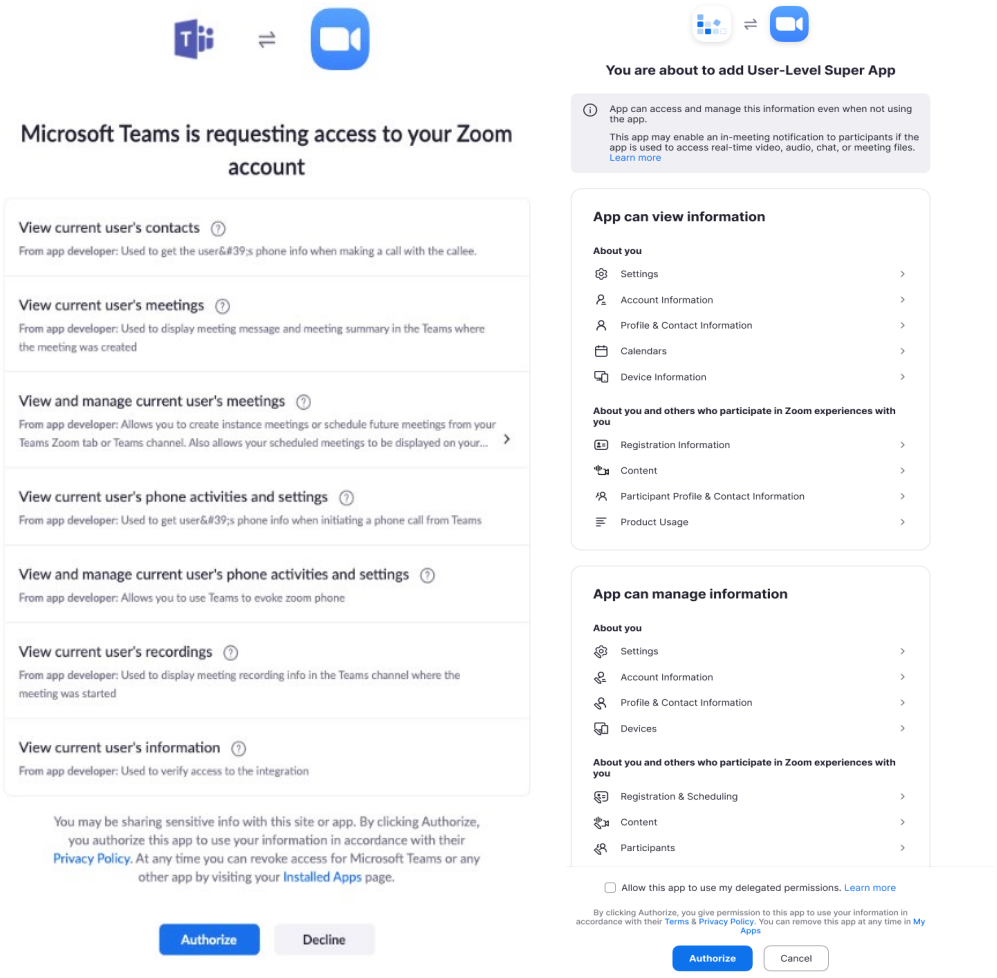
Zoom also gives users a choice if they want to give third parties access to their Zoom Account via the API. See Figure 15 below.

Users may want to give such access, or otherwise integrate third party apps, if they for example want to authorize a chatbot to send messages on their behalf in Zoom. Access to the API is turned Off by default. Even if the admin permits the use of the API, the user needs to authorise any permissions asked by third party applications.

[59] Zoom, Changing settings in the desktop client/mobile app, last updated 15 December 2021, URL: https://support.zoom.us/hc/en-us/articles/201362623-About-Settings.

[60] Zoom, End-to-end (E2EE) encryption for meetings, last updated 14 January 2022, URL: https://support.zoom.us/hc/en-us/articles/360048660871-End-to-end-E2EE-encryption-for-meetings.

Figure 15: Request for permissions third party app[61]



4.1.3. Privacy choices and default settings for Hosts

Zoom offers separate data protection controls to users when they act as host:

- Access security options via the security icon in the toolbar for quick access to essential in-meeting security controls.
- Create a custom (privacy) disclaimer when users join a meeting or sign-in to their account[62]
- Add a Feedback tab to the Windows Settings or Mac Preferences
- Use Focus mode, giving participants view of videos without seeing each other[63]
- Allow meeting participants to send a message visible to all participants (default On)

[61] Screenshot made in the browser access to Zoom.

[62] Zoom, Creating a Zoom custom disclaimer, 13 December 2021, URL: https://support.zoom.us/hc/en-us/articles/360051221831.

[63] Zoom, Using focus mode, 19 December 2021, URL: https://support.zoom.us/hc/en-us/articles/360061113751.

- Prevent participants from saving chat (default Off)
- Lock the meeting: When a host locks a Zoom Meetings that is already started, no new participants can join, even if they have the meeting ID and passcode (if the host has required one).
- Put participants on hold: Hosts can put an attendee on hold and their video and audio connections will be disabled momentarily.
- Remove participants: From that Participants menu, hosts can mouse over a participant's name, and several options will appear, including "Remove".
- Report a user: Hosts/co-hosts can report users to Zoom's Trust & Safety team.
- Disable video: Hosts can turn someone's video off (default Off).
- Mute participants: Hosts can mute/unmute individual participants or all of them at once. There is an option to 'Mute (everybody) Upon Entry' (default Off).
- Turn off file transfer: In-meeting file transfer allows people to share files through the in-meeting chat (default On)
- Turn off annotation: Hosts can disable the annotation feature in their Zoom settings to prevent people from writing all over the screens (default On)
- Disable private chat: Zoom has in-meeting chat for everyone, or participants can message each other privately. Hosts can restrict participants' ability to chat amongst one another (default On).
- Control screen sharing: The meeting host can turn off screen sharing for participants (default On).
- Control recording: The ability to record to the cloud or locally is something an account admin can control. If enabled, the host can decide to enable/disable a participant or all participants to record.

Zoom also offers some other privacy relevant security settings to Hosts:

- Waiting Room (default Off. When turned On, the Host has to admit participants individually and users cannot join before the Host has started the meeting)
- Require a passcode when scheduling new meetings (default On)
- Require a passcode for instant meetings (default On)
- Require a passcode for Personal Meeting ID (PMI) (default Off)
- Only authenticated users can join meetings (default Off – depends on the permissions set by admins)
- Only authenticated users can join meetings from Web client (default Off – depends on the permissions set by admins)

4.1.4. Privacy choices and default settings for users when they participate in a meeting

When participating in a session, individual users have access to and can modify their username, alias, contact information, and organisation name, and they have the option to include a photo. They also have the option to disable their camera and microphone features if they do not wish to make their picture or voice available to the rest of the participants.

4.2. Privacy controls for admins

Administrators of Zoom Meetings Enterprise can exercise control over the data processing by Zoom in multiple ways. In the initial DPIA a list was included of missing privacy controls. Some of these options were available for hosts of meetings, but a university or government organisation may want to take technical measures to prevent hosts from violating privacy and security rules, for example for all or specific groups of employees or students.

In reply to the initial DPIA Zoom explained that many of these controls were already available. In some other cases, Zoom's change to a role as data processor for all personal data removed the need for specific admin controls. Below, 18 different relevant options are discussed, with references to Zoom's documentation how to effectuate the setting.

4.2.1. Enable E2EE

Admins can enable end-to-end encryption for all Meetings. This is possible for all clients, except when Zoom is used via the browser. E2EE meetings are limited to 200 participants.

Admins can make E2EE mandatory for all users in their account, by clicking the lock icon, and then clicking *Lock* to confirm the setting.

Because Zoom can no longer see the contents of exchanged communications, the following functionality will no longer work:

- Join the meeting by telephone
- Join before host
- Cloud recording
- Live streaming
- Live transcription
- Breakout Rooms
- Polling
- Zoom Apps[64]

[64] Zoom, End-to-end (E2EE) encryption for meetings, last updated 14 January 2022, URL: https://support.zoom.us/hc/en-us/articles/360048660871-End-to-end-E2EE-encryption-for-meetings.

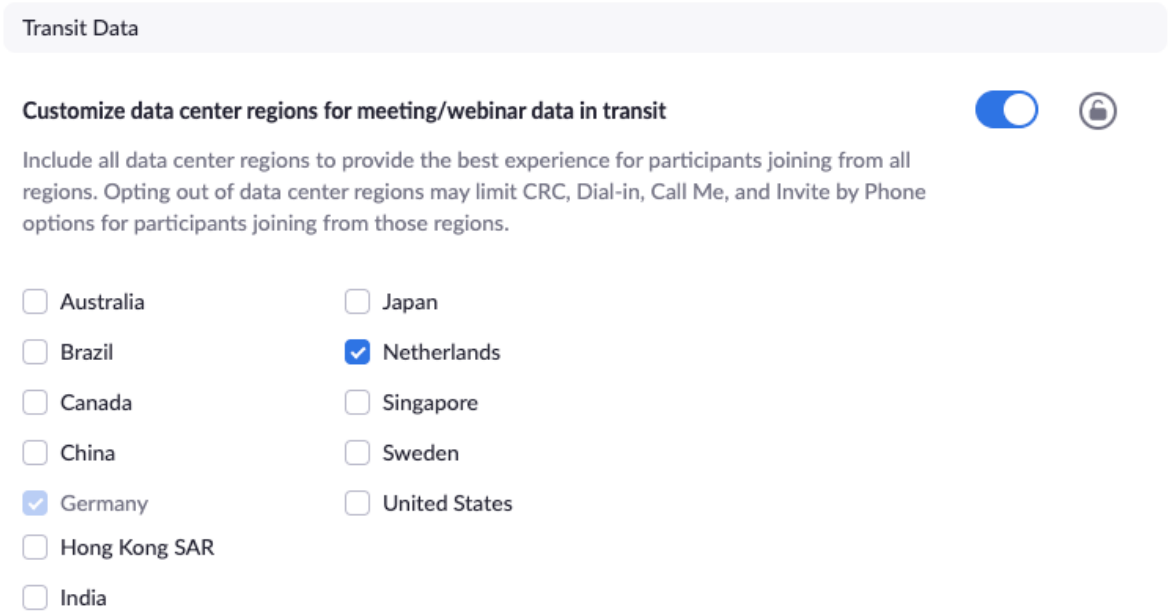
With up-to-date end user clients, the functionalities of meeting reactions and 1:1 Private Chats do still work. Admins can use local recording for Meetings.[65]

4.2.2. EU Geolocation

Until Zoom has completed its EU Cloud (by the end of 2022) admins should use the option to have all streaming and stored Content Data processed in Zoom's EU data centres (in Germany and the Netherlands, see Figure 16 below). This setting applies to all data exchanged in Meetings, recorded data such as cloud recordings and meeting transcripts, as well as files that are exchanged during a meeting.[66]

By mid-2022 Zoom commits to offer a choice to have all Support Data processed during EU business hours by its Romanian subprocessor, in the EU. Once that choice is active, admins will see an option to provide specific consent if they want to authorise Zoom to transfer incidental support requests to its subprocessors in the Philippines and the USA, when an organisation needs urgent support outside of EU working hours.

Figure 16: Zoom option to customize available data center regions for streaming data[67]



4.2.3. Public and private chat

Admins can enable or disable chat for all users in the account or for specific groups in the account.

[65] Zoom, Enabling and starting local recordings, last updated 23 January 2022, URL: https://support.zoom.us/hc/en-us/articles/201362473-Enabling-and-starting-local-recordings.

[66] Zoom, FAQS: Transferring EEA & UK Residents' Data to the US, URL: https://zoom.us/docs/doc/EEA_Transfer_of_Data.pdf. Zoom refers to these FAQs in its Answers to DPIA questions from 23 November 2020.

[67] Idem.

Admins can also disable private chat, which prevents participants from sending private messages to other participants in the meeting. Participants will still be able to privately message with the host. [68]

4.2.4. Enable Advanced chat encryption

Admins can enable Advanced chat encryption. Zoom explains: "*When advanced chat encryption is enabled, Content Data at rest is encrypted by keys generated & operated on chat participants' devices.*" [69]

4.2.5. Use of SSO and Vanity URL

Organisations can deploy SSO for employees to subscribe to Zoom, with an organisational subdomain. [70] Such a Vanity URL [71] creates three privacy controls:

Use email aliases. Zoom explains: "*In most email systems it is possible to create multiple aliases for each user that are routed to the same user inbox. Customers can thus create an alias for each of their users to ensure that they are not easily identifiable by their email address. An admin can choose to only provide these pseudonymous addresses to Zoom.*"

Remove or replace first name and surname. Zoom explains it does not need the full name of the user to provide its services. "*The customer can decide to delete these data from existing accounts, use a generic organisation name (*such as: *University of Amsterdam*, example added by Privacy Company*) and/or not to provide any details for new users. The service will still work, even though the display name may be blank/anonymised. This may make existing waiting room functionality hard, but video waiting rooms would mitigate this.*" [72]

Prevent use of cookies and transfer of IP addresses and device identifiers of end users to the USA when they look up information on Zoom's publicly accessible website. Traffic to an EU Customer's Vanity URL stays within the EU.

4.2.6. Prevent participants from saving chats

Chats are automatically saved. Organisations may want to disable this feature and prevent participants from saving chats that may contain personal data, not just from participants, but also remarks about, or data from, other individuals. [73]

---

[68] Zoom, Enabling or disabling in-meeting chat, last updated 15 December 2021, URL: https://support.zoom.us/hc/en-us/articles/115004809306-Enabling-or-disabling-in-meeting-chat.

[69] Zoom, Advanced chat encryption, 1 February 2022, URL: https://support.zoom.us/hc/en-us/articles/207599823.

[70] Zoom, Quick start guide for SSO, last updated 15 December 2021, URL: https://support.zoom.us/hc/en-us/articles/201363003-Quick-start-guide-for-SSO.

[71] Zoom, Guidelines for Vanity URL requests, Last updated 9 April 2021, URL: https://support.zoom.us/hc/en-us/articles/215062646-Guidelines-for-Vanity-URL-Requests.

[72] Zoom reply to part A of the DPIA, 19 March 2021, p. 16.

[73] Zoom, (Disabling) auto saving chats, last updated 11 January 2022, URL: https://support.zoom.us/hc/en-us/articles/360060889932-Enabling-auto-saving-chats.

4.2.7. Sharing of data in chats

Admins can set limits to the type and size of files that can be shared in chats:

- Only allow specified file types (optional): Specify the file types that users can send in chat. Zoom desktop client version 5.4.0 or higher is required.
- Maximum file size (optional): Specify the maximum file size (MB) that users can send in chat and in-meeting chat. Zoom desktop client version 5.4.0 or higher is required."[74]

4.2.8. Do not enable Attendee Feedback

As described in Section 1.7 Zoom has disabled this survey request by default for its EU Education and Enterprise customers.[75] As the survey contains an open text field, there is a possibility that end users provide personal data in this text box. To mitigate this risk, Zoom has disabled this functionality by default.

4.2.9. Do not enable Giphy

The US based company Giphy enables users to search for illustrations based on keywords, based on its archive of millions of GIFs, stickers, and video clips/animations. Facebook bought Giphy in May 2020. If the organisation has enabled advanced chat encryption, use of Giphy is technically impossible. To prevent traffic to Giphy/Facebook as a third party (Zoom does not have a subprocessor agreement with Giphy or Facebook) admins should not enable this integration in the Zoom chats.[76]

4.2.10. Mute individual or all participants upon entry

This meeting setting can help manage participants and prevent distractions and interruptions during a meeting (Zoom-bombing).[77]

4.2.11. File transfer

To prevent accidental data breaches, file transfer is disabled by default.[78]

---

[74] Zoom, Sharing, URL: https://support.zoom.us/hc/en-us/articles/203749815#h_01EH3B3FMB1ZRY9RF5Z1RJSMQV.

[75] Zoom, End-of-meeting experience feedback survey, 11 January 2022, URL: https://support.zoom.us/hc/en-us/articles/115005855266-End-of-meeting-experience-feedback-survey.

[76] Zoom, Managing IM groups, last updated 13 December 2021, URL: https://support.zoom.us/hc/en-us/articles/203749815.

[77] Zoom, Muting all participants when they join a meeting, last updated 15 December 2021, URL: https://support.zoom.us/hc/en-us/articles/360060860512-Muting-all-participants-when-they-join-a-meeting.

[78] Zoom, Sending a file in meetings and webinars, last updated 15 December 2021, URL: https://support.zoom.us/hc/en-us/articles/209605493-Sending-a-file-in-meetings-and-webinars.

4.2.12. Annotation

Enabling annotation tools allows meeting participants to collaborate, brainstorm, and draw over shared content. This functionality is disabled by default.[79]

4.2.13. Prohibit the viewing and recording of the 'gallery' during screen sharing

Admins can prohibit viewing and recording of the gallery with participants when a screen is shared, by selecting active speaker view. This means the teacher can see the students, but the students do not see each other, nor are they recorded. This helps guarantee the public character of meetings and recordings.[80]

4.2.14. Visibility of participants

Admins can allow users to see each other's contact details, depending on classification in one of three visibility groups. Zoom explains:

- Private: Only members can see the group automatically. Users who are not in the group can search for users who are in the group.
- Shared: All people in the account can see the group and members automatically.
- Restricted: No one can see the group or find the members of the group using search except for those in the group."[81]

4.2.15. Co-hosts

There is a control for co-hosts. The admin can use this to enable hosts to add co-hosts. Co-hosts have the same in-meeting controls as the host.[82]

4.2.16. Polling

With the control for polling, the admin can add 'Polls' to the meeting controls. This allows hosts to survey the attendees.[83] As shown in Appendix 1 the surveys involve the use of a cookie from the US based company Wootric, and hence, traffic with a.o. IP addresses to the USA. The company is included in the list of authorised subprocessors from Zoom, and thus bound to the same data protection guarantees as Zoom itself.

---

[79] Zoom, Enabling or disabling annotation tools for meetings, last updated 10 December 2021, URL: https://support.zoom.us/hc/en-us/articles/4409894568845-Enabling-or-disabling-annotation-tools-for-meetings.

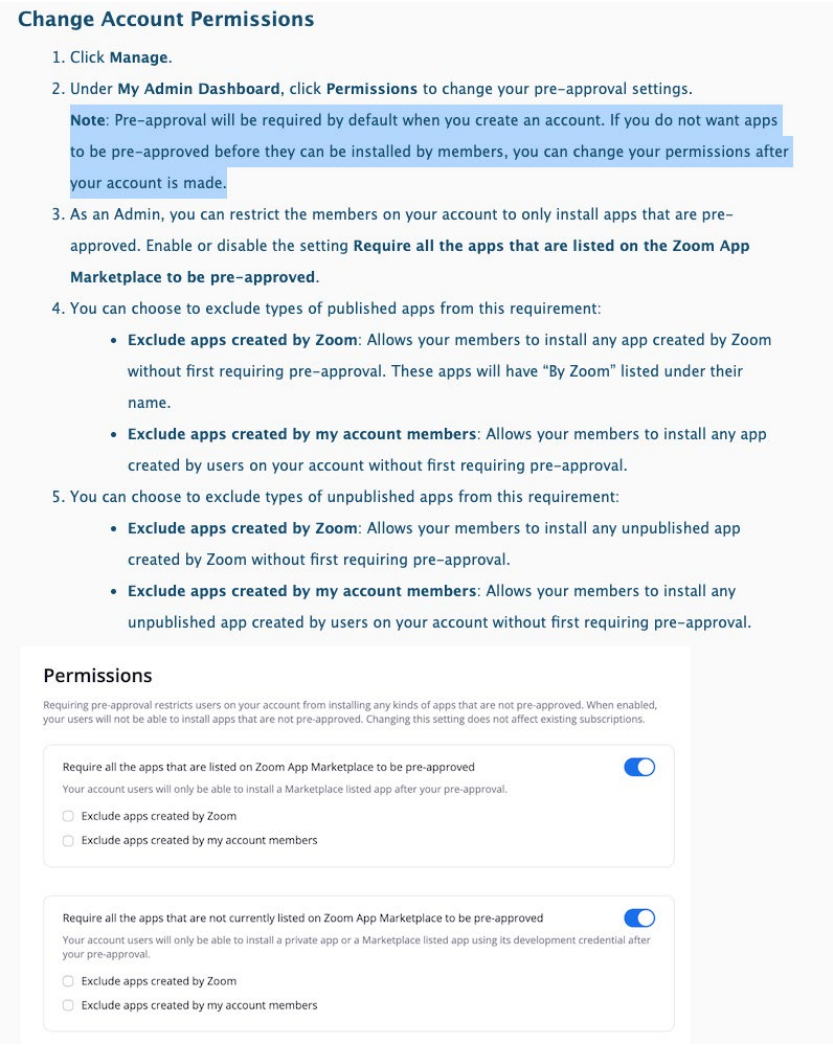
[80] Zoom,. Adjusting your video layout during a virtual meeting, URL: https://support.zoom.us/hc/en-us/articles/201362323-Adjusting-your-video-layout-during-a-virtual-meeting.

[81] Zoom, Managing IM groups, Last Updated 13 December 2021, URL: https://support.zoom.us/hc/en-us/articles/203749815.

[82] Zoom, Host and co-host controls in a meeting, last updated 21 January 2022, URL: https://support.zoom.us/hc/en-us/articles/201362603.

[83] Zoom, Enabling polling for meetings, last updated 15 December 2021, URL: https://support.zoom.us/hc/en-us/articles/4412324684685.

Figure 17: Zoom explanation about account permissions for apps[84]



4.2.17. API features and Marketplace apps

An admin has access to a number of API features. Access to the API is turned Off by default. This means the admin has to pre-approve use of all apps in the Marketplace. There is an option for admins to enable API access to all users' chat messages in this account. By default, the admin has to approve all authorisation requests from end-users (See Figure 17 above).

4.2.18. Integration of user calendar and contacts

Zoom account administrators can enable users to integrate their calendar and contacts. Zoom supports Google Calendar, Microsoft Exchange and Microsoft Office 365. This is a relevant privacy choice, as these Content Data fall outside of the subset of Content Data for which admins can determine that they may only be stored in the EU (in Germany). This will change after the end of 2022,

[84] See also Zoom, Managing the Zoom App Marketplace, last updated 3 February 2022, URL: https://support.Zoom.us/hc/en-us/articles/360032447812-Managing-Zoom-Marketplace.

when Zoom processes all personal data of its EU Education and Enterprise customers exclusively in the EU.

5. Purposes of the processing

Under the GDPR, the principle of 'purpose limitation' dictates that personal data may only be collected for specified, explicit and legitimate purposes, and may not be further processed in a manner that is incompatible with the initial purpose.[85] The purposes are qualified and assessed in part B of this DPIA. This Section does not repeat the initial very long (and confusing) list of purposes for the different categories of personal data in the first DPIA. This list was distilled from different legal sources, and expanded after Zoom drafted its first Privacy Data Sheet. This list no longer applies since Zoom has decided to factually and contractually become a data processor for all personal data (except the public website). The agreed limited purposes are described in Section 5.2 below.

5.1. Purposes universities and government organisations

The general interests government organisations may have to use Zoom Meetings are described in Section 7.1.

Organisations may process Diagnostic Data collected by Zoom about the individual use of the videoconferencing services when accessing or retrieving data from the available meeting and operator log files. Organisations need to have access to these data to comply with information security requirements, to verify access authorisations, to investigate and mitigate data security breaches and to comply with data subject right requests.

As data controllers, universities and government organisations must determine when they need to access log files generated by Zoom, what retention periods are necessary to comply with their specific security requirements or legal retention obligations, and for what specific purposes specific personal data in the log files may be (further) processed and analysed. These specific purposes are not in scope of this umbrella DPIA.

5.2. Purposes Zoom

In its new Data Processing Agreement for EU Enterprise and Education customers, Zoom defines two different sets of purposes, depending on its role as processor or as (authorised) independent controller.

5.2.1. Purposes Zoom as a processor

Zoom may process the personal data for five purposes, only to the extent necessary and proportionate:

[85] Article 5(1)(b) GDPR.

1. Providing and updating the Services as licensed, configured, and used by Customer and its users, including through Customer's use of Zoom settings, administrator controls or other Service functionality.
2. Securing and real-time monitoring the Services.
3. Resolving issues, bugs, and errors.
4. Providing customer requested support, including applying knowledge gained from individual customer support requests to benefit all Zoom customers but only to the extent such knowledge is anonymised.
5. Processing as set out in the Agreement and Annex I to the SCCs detailing the subject matter, nature, purpose, and duration of Personal Data Processing in the controller to processor capacity and other documented instruction provided by Customer and acknowledged by Zoom as constituting instructions for purposes of this Data Processing Agreement.[86]

These five purposes are explained in more detail below. Though the descriptions may seem broad at first sight, they are limitative.

Securing the services

In *Annex II: Technical and Organizational Security Measures* appended to the Zoom DPA; Zoom provides extensive information about its security purposes. Zoom describes policies and processes to secure Content Data. This description includes a number of scenarios where Zoom may process Customer Data (including personal data) specifically for the purpose of securing the data against *vulnerabilities, existing and emerging threats and actual attacks*.

This may involve using malware detection tools in its production environment. "*In production, Zoom must employ tools to detect, log and disposition malware.*"[87] In reply to this DPIA, Zoom confirmed that it does not use third party tools for this purpose.[88]

Zoom also processes personal data for the purpose of Intrusion Detection/Advanced Threat Protection. Zoom writes: "*Network and host-based intrusion detection/advanced threat protection must be deployed with events generated fed into centralized systems for analysis. These systems must accommodate routine updates and real-time alerting. IDS/advanced threat protection signatures must be kept up to date to respond to threats.*"[89]

Zoom has explained its use of monitoring and logging tools to centralize security events for analysis and correlation. With respect to Intrusion Detection and Incident Response, like any other service provider Zoom keeps logs in its own monitoring files (SIEM). Zoom has explained it retains log files from its S3-buckets from AWS, and unstructured metadata for this purpose, but these logs generally do not contain personal data relating to customers.

[86] Zoom DPA, Clause 2.2

[87] Zoom DPA, Annex II, 18 *Vulnerability Monitoring*

[88] Zoom reply to part A of the DPIA, 19 March 2021, p. 53.

[89] Zoom DPA, Annex II, 18 *Vulnerability Monitoring*.

Zoom explained in the context of this DPIA it uses a third-party vendor to perform annual penetration tests of the production networks.[90] Zoom explains: "*The vendor(s) assess(es) the Zoom system perimeter and configurations, and on occasion example images of systems. The vendor(s) do not directly connect to Zoom systems that hold customer data, nor can the vendors assess or review the data held in such systems.*"[91] That is why such vendors are not separately mentioned in the list of subprocessors for the EU Education and Enterprise customers' personal data.

Providing support

Zoom has explained that this purpose means: "*to troubleshoot and diagnose Service problems, route support requests, repair devices and to provide customer care and support services. This includes enabling Zoom to provide, improve and secure the quality of Zoom Services and to investigate security incidents, as well as for our internal auditing of the effectivity of our support process and updating our guidance and support pages.*"[92] Via this purpose, Zoom is explicitly authorised to anonymise Support Data to improve the support for all Zoom customers.

5.2.2. Compatible purposes Zoom as a data controller

Additionally, the DPA authorises Zoom to 'further' process some personal data it obtains in its role as processor, for its own legitimate business purposes. Zoom may only process personal data for these purposes when the processing is strictly necessary and proportionate, and only for the following exhaustive list of purposes:

Directly identifiable data (name, screen name, profile picture and email address and all Customer Personal Data (as defined in Section 1.1) directly connected to such directly identifiable data) for:

1. billing, account, and customer relationship management (marketing communication with procurement/sales officials), and related Customer correspondence (mailings about for example necessary updates).
2. complying with and resolving legal obligations, including responding to Data Subject Requests for Personal Data processed by Zoom as data Controller (for example Website Data), US tax requirements, agreements and disputes.
3. abuse detection, prevention and protection (such as automatic scanning for matches with identifiers of known Child Sexual Abuse Material ("CSAM"), virus scanning and scanning to detect violations of terms of service (such as copyright infringement, SPAM, and actions not permitted under Zoom's Community Standards (also known as an acceptable use policy).

Pseudonymised and/or aggregated data (Zoom will pseudonymise and/or aggregate as much as possible and pseudonymised and/or aggregated data will not be processed on a per-Customer level) for:

[90] Zoom Answer to DPIA questions, 23 November 2020, answers to Q4f.

[91] Zoom reply to part A of the DPIA, 19 March 2021, p. 53.

[92] Zoom reply to part A of the DPIA, separate spreadsheet, 19 March 2021.

4. improving and optimizing the performance and core functionality of accessibility, privacy, security and IT infrastructure efficiency of the Services, including zoom.us, explore.zoom.us and support.zoom.us.
5. internal reporting, financial reporting, revenue planning, capacity planning and forecast modelling (including product strategy).
6. receiving and using Feedback for Zoom's overall service improvement (when enabled by admins).[93]

These purposes are limitative. They have all been minutely discussed and defined in dialogue with Zoom. The scope is explained in more detail below.

Billing and mailing

For the first purpose of 'billing' and 'account management' Zoom processes Diagnostic Data "to authenticate users to the platform and enforce payment plans, such as tracking usage for Cloud recording accounts that pay by gigabytes per month." [94]

The first purpose authorises Zoom to send commercial messages to its commercial contacts, but conversely, prohibits the sending of commercial mails to the admins and end users. Zoom may only send necessary non-commercial communication to these accounts. Zoom explained: "*As a rule, Zoom does not contact non-account holder/non-administrator members of an Enterprise account. I do not know of actual instances where Zoom has relied on this clause, but I could imagine it might be relevant if we needed to meet a legal obligation, such as a data breach requirement.*"[95]

Compliance with legal obligations, incl. US surveillance

One of the most difficult purposes to understand and define is *compliance with legal obligations* in the second purpose. In Section 6.3.1 a table is included with all known US law enforcement and national security powers that may be used to compel Zoom to disclose personal data from European end users. The ensuing data transfer risks are discussed in Section 8.

Another relevant legal obligation is US fiscal law. In September 2020, new US fiscal law entered into force with new requirements for companies that provide electronic services to provide evidence of the origin of their income. In order to shift taxation from the US to a European country (deduct Foreign-Derived Income), providers have to provide evidence of foreign derived income by retaining the IP addresses of the end users in the EU for a period between 3 and 6 years. This follows from Treasury Regulation 1.250(b)-5(e) for services provided to businesses.

"*If the location of access cannot be determined (such as where the location of access cannot be reliably determined using the location of the IP address of the device used to receive the service), (…) if gross*

[93] Zoom new DPA, Section 2.4.

[94] Zoom Answers to DPIA questions, answer to Q4i.

[95] Idem, p. 22.

receipts are at or above this $50,000 threshold, the business recipient's operations that benefit are deemed to be located in the United States."[96]

In dialogue with SURF, Zoom is seeking third-party support for an alternative solution that will remove the necessity of retaining the actual IP addresses.

Scanning for CSAM

Another specific US legal obligation is the requirement for US communication providers to *detect and report Child Sexual Abuse Material (CSAM)* as defined in the third purpose. The second purpose of compliance with legal obligations includes the scanning of Content Data for (CSAM). This involves the use of a scanning tool, and the automated transfer of 'hits' to the US based National Center for Missing & Exploited Children. This is a private, non-profit 501(c)(3) corporation based in the USA, whose mission is to help find missing children, reduce child sexual exploitation, and prevent child victimization.[97]

Zoom explains that it uses Microsofts PhotoDNA image scanning tool for this purpose: "*This tool automatically detects and report child sexual abuse material on different parts of our platform such as chat, file uploads, profile pictures and room backgrounds. Such images will be automatically blocked and reported to NCMEC through the API. For more information see https://www.microsoft.com/en-us/photodna.*"[98] Zoom also explained there is no feedback loop or other transfer of personal data to Microsoft.

Zoom uses PhotoDNA to scan three types of Content Data:

1. persistent chat file uploads (that is, files exchanged in the persistent chat function, separate from the in-meeting chat function),
2. Zoom Room backgrounds, and
3. avatars.

Zoom has assured that Microsoft's PhotoDNA only reports 'hits' when there is an absolute match with the fingerprint of 'known' CSAM. The tool does not use artificial intelligence to predict possible matches.

Zoom adds: "*If PhotoDNA detects an illicit image, Zoom will immediately suspend the account responsible, generate a report to review by Zoom's Trust and Safety Team, and escalate to the appropriate child protection agency if necessary. PhotoDNA is not facial or object recognition technology. A PhotoDNA signature cannot be used to recreate an image or identify people or items*

[96] See the text of this Regulation at https://casetext.com/regulation/code-of-federal-regulations/title-26-internal-revenue/chapter-i-internal-revenue-service-department-of-the-treasury/subchapter-a-income-tax/part-1-income-taxes/computation-of-taxable-income/special-deductions-for-corporations/section-1250b-5-foreign-derived-deduction-eligible-income-fddei-services and the explanation by the US Internal Revenue Service, Deduction for Foreign-Derived Intangible Income and Global Intangible Low-Taxed Income, effective date 14 September 2020, URL: https://www.federalregister.gov/documents/2020/07/15/2020-14649/deduction-for-foreign-derived-intangible-income-and-global-intangible-low-taxed-income.

[97] URL: https://www.missingkids.org/footer/about.

[98] Zoom Answers to DPIA questions, 23 November 2020, Answer to Q4d.

within an image. It can only be used to identify copies of known CSAM, for which NCMEC has assigned a PhotoDNA signature." [99]

Zoom has created an API integration with NCMEC. Zoom explains: "*Our internal dashboard will be integrated with the NCMEC API, which enables automated reporting via our dashboard and other tools (like PhotoDNA) directly to NCMEC in order to build upon our existing work on child safety.*"

Zoom cannot delay this automated reporting. However, to mitigate the risks of incorrect profiling of an end user as involved with CSAM, Zoom has contractually committed to perform a human review before the account is terminated. In that case, the user will see a pop-up that the account is blocked, with a possibility to appeal the decision, via https://zoom.us/appeals.

Detecting violations of the Community Standards

Related to this scanning is Zoom's right to process personal data for the purpose of detecting actions not permitted under *Zoom's Community Standards*. This policy is included in the DPA in Exhibit B. The DPA stipulates: "*Customer shall not provide or make available to Zoom any Customer Personal Data in violation of the Agreement, this Addendum, or otherwise in violation of Zoom' s Community Standard's in Exhibit B, and shall indemnify Zoom from all claims and losses in connection therewith.*" [100]

In reply to questions in the context of the DPIA, Zoom explained that it primarily responds passively to user complaints about Prohibited Content. Zoom's Trust & Safety Team in the USA processes complaints and reports about abusive behaviour and/or sharing of prohibited content such as swastikas or CSAM. Such complaints may also relate to spam or signals that the security of an account is possibly breached, for example if an end user signs in from multiple locations simultaneously. If Zoom wants to prohibit a confirmed bad actor from reconnecting to the service it needs to take into account that that person may try to reconnect with a different device, different IP address and/or different name. Therefore, the Trust & Safety Team creates a new pseudonymous unique identifier with all available information from the service generated server logs. Zoom explains it creates: "*a Zoom persistent unique identifier that Zoom's Trust and Safety Team combines with other data elements including IP address, data center, PC name, microphone, speaker, camera, domain, hard disc ID, network type, operating system type and version, and client version. Zoom uses this data to identify and block bad actors that threaten the security and integrity of Zoom Services. This data is accessible only by Zoom employees with a need to know and subject to appropriate technical and organizational measures.*" [101]

Improving and optimizing

In reply to questions about the fourth purpose, with the very broad terms '*improving and optimizing*' Zoom explained that optimization of the services means use of the data "*to help the services run most efficiently, for example, balancing network load*." [102]

---

[99] Zoom reply to part A of the DPIA, 19 March 2021, p. 54.

[100] Zoom DPA, Clause 2.10.

[101] E-mail Zoom to SURF, 3 February 2022.

[102] Ibid. Zoom Answers to DPIA questions, answer to Q4i.

Further processing of aggregated data

For the fourth and fifth purpose, Zoom is not permitted to use directly identifiable data, but must aggregate, and may not process data on a per-Customer level. This is an important guarantee to protect the confidentiality of the use of Zoom services. The first DPIA flagged a misunderstanding about the level of aggregation. Initially, Zoom mentioned the following example of aggregation:

"*Our Data Science teams follow guidelines that prohibit the production of reports or data products that identify individual account members that are not the Enterprise Account Owner (business contact) or Administrator(s). For example, the data Science team produces a report that shows customers with very high percentages of undeployed licenses, e.g., 85% undeployed. The Customer Success Manager for that customer will then have access to the contact details for that Account owner and admin so they can contact them to offer deployment support.*"[103]

The example showed that Zoom permitted itself to perform analyses of uptake or usage at an individual Education or Enterprise customer level. Zoom did not provide a definition and did not specifically exclude other types of analyses that could be performed at an individual customer level that would potentially be more invasive (for example, average time spent in Meetings per day of the week by users of a specific organisation).

If Zoom processes personal data to create aggregated, pseudonymised or anonymised datasets for this purpose, this still qualifies as processing of personal data, for which Zoom and/or the Dutch universities and government organisations need to have a legal ground. Section 9.3 of this report outlines some of the requirements for successful anonymisation of data.

Feedback

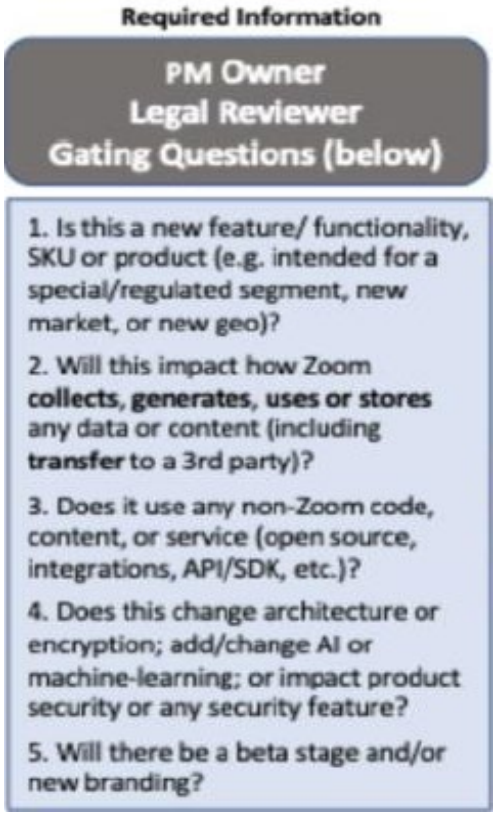
If admins enable Feedback, or end users voluntarily provide input to a Feedback form, Zoom may use the anonymised, aggregated analytics for its overall service improvement. Such analytics will never reveal customer-specific data, but are conducted at a higher aggregation level. Zoom also provides the feedback in aggregated reports to the admins.

Internal enforcement of purpose limitation

Zoom has explained how it guarantees internally that personal data from its EU Enterprise and Education customers are only processed for these authorised purposes. Zoom has a policy and processual rules to apply privacy by design to all new or changed data processing. This means security and privacy officials have to sign off on proposed new data processing before it can be entered in production. At the request of SURF, Zoom has agreed to have its compliancy with these and other data protection policies and rules verified in a SOC-2 audit, in which the 'Privacy' controls will be added.

[103] Zoom reply to part A of the DPIA, 19 March 2021, p. 57.

Figure 18: Zoom internal mandatory Privacy by Design questions



6. Processor or (joint) controller

This section assesses the data protection role of Zoom and its customers (the universities and government organisations) in the context of the Zoom Meetings Enterprise services.

6.1. Definitions

The GDPR contains definitions of the different roles of parties involved in processing data: (joint) controller, processor and subprocessor.

Article 4(7) of the GDPR defines the (joint) controller 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; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.*"

Article 26 of the GDPR stipulates that where two or more data controllers jointly determine the purposes and means of a processing, they are joint controllers. Joint controllers must determine their respective responsibilities for compliance with obligations under the GDPR in a transparent manner, especially towards data subjects, in an arrangement between them.

Article 4(8) of the GDPR defines a processor as:

"a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller." A subprocessor is a subcontractor engaged by a processor that assists in the processing of personal data on behalf of a data controller.

Article 28 GDPR sets out various obligations of processors towards the controllers for whom they process data. Article 28(3) GDPR contains specific obligations for the processor. Such obligations include only processing personal data in accordance with documented instructions from the data controller and cooperating with audits by a data controller. Article 28(4) GDPR stipulates that a data processor may use subprocessors to perform specific tasks for the data controller, but only with the prior authorisation of the data controller.

When data protection roles are assessed, the formal contractual division of roles is not leading nor decisive. The actual role of a party must primarily be determined on the basis of factual circumstances.

6.2. Data processor

Pursuant to the new Zoom DPA, Zoom is data processor for the processing of all personal data, as defined in the term 'Customer Personal Data' quoted in Section 2.2.3.

Zoom's DPA states: "*Customer is the Controller of Customer Personal Data. Zoom is the Processor of Customer Personal Data, except where Zoom or a Zoom affiliate acts as a Controller processing Customer Personal Data in accordance with the exhaustive list of Legitimate Business Purposes in Section 2.4.*"[104]

To technically provide the remote conferencing services, and to keep the service secure, well-functioning and bug free, Zoom necessarily needs to process the streaming Content Data, and some Diagnostic Data about the individual use of the services. To provide support and to execute the instructions from its customers to deliver the requested services, Zoom must also process Account, Support and Website Data.

In order to achieve its objectives, the data processor has a certain liberty to decide how the personal data are processed and in which systems (with which means). However, the processor must be transparent about the personal data it needs to process, and for what purposes, in order to successfully claim to act on instructions of the controller.

Data controllers must determine the purposes of processing in a data processor agreement with the data processor. Data processors may only process personal data on behalf of the data controller. As quoted above in Section 5.2.1, the new Zoom DPA contains five clear purposes. These purposes are therefore part of the government and universities' documented instructions.

Through this limitative list of purposes, with the explanations of their impact, Zoom enables universities and government organisations to verify their compliance with the obligation as data controllers to only process personal data for specific and explicit purposes.

The new Zoom DPA also contains a list of six additional purposes, for which Zoom may process some personal data for its own legitimate business purposes. These purposes are discussed in Section 6.3 below. This list of legitimate business purposes requires some explanation. Legally, a data processor

[104] Zoom DPA, Clause 2.1.

may not determine what purposes it finds compatible with the main purpose of technically providing the contracted software or services. If a processor determines any purposes of processing, it becomes a data controller. In that case it violates its obligations as a data processor, as explained in Art. 28(10) of the GDPR: "*if a processor infringes this Regulation by determining the purposes and means of processing, the processor shall be considered to be a controller in respect of that processing.*"

However, in practice it is inevitable that a company that collects and generates personal data as a data processor must process some of these personal data for its own business purposes. For example, use Account Data to send invoices for provided services and include statistics in financial reports, or process Diagnostic Data by aggregating them to forecast necessary future network capacity.

The French National Supervisory Authority CNIL has recently published a useful explanation of how data controllers can allow data processors to process personal data for these necessary operations.[105]

The CNIL explains that a processor may *further* process data as an independent data controller, provided that the controller has assessed the processing is compatible, and that the controller explicitly authorises the processor in writing to process for these purposes. The CNIL writes [informally translated]:

"A data processor may only reuse personal data on its own behalf if such reuse is compatible with the initial processing and if the controller has authorised this processing in writing. (…)

The controller may, under the conditions set out below, authorise its processor to reuse the personal data on its own behalf. The processor then becomes the data controller for this new processing. (…)

The data controller must determine whether such further processing is compatible with the purpose for which the data were originally collected, if the processing is not based on the data subject's consent or on a specific legal obligation."[106]

Therefore, the provisions in the DPA about processing for Zoom's legitimate business purposes do not prejudice Zoom's role as data processor.

In sum, as a result of the first DPIA and resulting negotiations with SURF, Zoom has changed its factual data processing and legally committed to a processor role in its new DPA. Legally and factually Zoom qualifies as a data processor.

6.2.1. Subprocessors

Through the new Zoom DPA, customers authorise (give prior written consent to) the limitative list of authorised subprocessors and Zoom affiliates attached to the Zoom DPA as Annex III. See Table 3 below. Zoom also publishes a list of the subprocessors and affiliates it engages.[107]

The Authorized Subprocessor is defined in the Zoom DPA as a "*Subprocessor engaged by Zoom to Process Customer Personal Data on behalf of the Customer per the Customer's Instructions under the*

[105] CNIL, Sous-traitants : la réutilisation de données confiées par un responsable de traitement, 12 January 2022, URL: https://www.cnil.fr/fr/sous-traitants-la-reutilisation-de-donnees-confiees-par-un-responsable-de-traitement.

[106] Idem.

[107] Zoom, Third-Party Subprocessors, effective 30 December 2021, URL: https://zoom.us/subprocessors.

terms of this Agreement and this Addendum. Authorized Subprocessors may include Zoom Affiliates but shall exclude Zoom employees, contractors and consultants."[108]

Table 3: Zoom list of authorised subprocessors for EU Enterprise and Education customers[109]

Subprocessor	Purpose	Category of personal data	Location	Type of agreement and date signed
Amazon Web Services	Cloud Service Provider	● Real-time meeting and webinar traffic ● Meeting and call recordings (if saved to the cloud by Customer ● Transcriptions of meeting or call recordings (if meeting recorded and saved to the cloud by Customer) ● Uploaded files	United States, E.U., Canada, Australia	SCCs
Oracle	Cloud Service Provider	● Real-time meeting and webinar traffic ● Meeting and call recordings ● Transcriptions of meeting or call recordings	United States	Binding Corporate Rules (BCRs) + new SCCs in progress
Google Firebase	Send push notifications on Android phones. Customers can choose not to use this service.	● Chat Message Notification ● SMS Message Notification ● PBX (Phone Call) Message Notification	United States	SCCs
Apple	Send push notifications on iOS phones. Customers can choose not to use this service.	● Chat Message Notification ● SMS Message Notification ● PBX (Phone Call) Message Notification	United States	SCCs
InMoment (Wootric)	Process survey responses post-meeting	The following personal data MAY be shared with InMoment but only if the Customer chooses to provide a survey response after the meeting. ● Name ● Email address ● Phone number ● Survey responses	United States, E.U., Australia	SCCs
Twilio	For webinars. Send notification emails to webinar	● Name ● Email address ● Meeting or webinar subject ● Meeting/webinar ID	United States	SCCs

[108] Zoom new DPA, Clause 1.2.

[109] Attached as Annex III to the DPA that is part of the contract with SURF for the Dutch universities.

	registrants with Webinar details.	● Meeting date and start time		
Zendesk	Cloud-based Customer Service Platform	Communications Content such as cloud recordings or in-meeting chat transcripts MAY be shared with Zendesk but only if Customer chooses to provide it directly to a Zoom support agent through a support interaction.	United States	BCRs) + new SCCs in progress
CSS Corp	Support Providers	Communications Content such as cloud recordings or in-meeting chat transcripts MAY be shared with CSS Corp but only if Customer chooses to provide it directly to a Zoom support agent through a support interaction	Romania	SCCs
TaskUS	Support Providers	Communications Content such as cloud recordings or in-meeting chat transcripts MAY be shared with TaskUS but only if Customer chooses to provide it directly to a Zoom support agent through a support interaction.	Philippines	SCCs
One Trust	Cookie Consent Management and Data Subject Access Request Platform	For the Cookie Consent Management: ● User cookie preference ● IP address ● Location (derived from IP address) For Data Subject Access Requests, the following data MAY be provided if Customer chooses to provide it when directing Zoom to fulfil a data subject access request via the OneTrust webform: ● Name ● Email address ● Plan type ● User role ● Country/state of residence	United States	SCCs

Zoom's affiliates are defined in the DPA as "*any entity that directly or indirectly controls, is controlled by, or is under common control with that party. For purposes of this Addendum, "control" means an economic or voting interest of at least fifty percent (50%) or, in the absence of such economic or voting interest, the power to direct or cause the direction of the management and set the policies of such entity*." The list of affiliates shows the list of Zoom offices across the globe. Zoom has explained to SURF that personal data from its EU Enterprise and Education customers are only processed by its affiliates when an individual Zoom user travels abroad, and uses his or her existing account to use Zoom services in that country.

This reassurance is included in Zoom's new DPA: "*Zoom may transfer Customer Personal Data to third countries (including those outside of the EEA without an adequacy statement from the European Commission) to Affiliates, its professional advisors or its Authorized Subprocessors when a Zoom End User knowingly connects to data processing operations supporting the Services from such locations (such as when the End user travels outside of the territory of the EU). Zoom shall ensure that such transfers are made in compliance with Applicable Data Protection Law and this Addendum.*"[110]

Zoom's DPA contains specific rules for the engagement of new third party subprocessors.

Zoom will inform the Customer about a new subprocessor (at least) 30 business days in advance. If the Customer wishes to object, Zoom offers 4 conflict resolution options:

1. Zoom will not let the new subprocessor process Customer's data,
2. Zoom will give new instructions to the new subprocessor to overcome Customer's objections,
3. Zoom may cease to provide, or the Customer may cease to use, the service that would involve engagement of the new subprocessor, or
4. Zoom will provide Customer with a commercially reasonable alternative for the engagement, or if the Customer does not agree either, to terminate the agreement.[111]

Through the DPA, Zoom binds its subprocessors to the same data protection obligations agreed with its customers, with the exception of the period for advance notification. Zoom is not in a position to force all of its subprocessors (including hyperscalers such as AWS, Google Firebase, Oracle and Apple) to honour the same period of 30 business days advanced notice if they deploy new sub-subprocessors. Therefore, the DPA specifies: "*The Parties acknowledge and agree that notice periods shall be deemed equivalent regardless of disparate notification periods.*"[112]

Explanations about specific subprocessors

Zoom explains it uses multiple data centres to ensure performance and availability, but the end user connects to the nearest data centre, in the same geolocation. Real-time Meeting data from EU end users are processed in AWS's and Oracle's EU data centres.

Zoom uses Zendesk as a subprocessor for its Support Services platform. This means all tickets (requests and answers) are processed with this tool. Zoom currently uses three subprocessors to provide the factual support, one in the EU (CSS Corp) and one in the USA and the Philippines (TaskUS).

Zoom has committed to create a separate Zendesk instance for Support Data from European organisations, by mid-2022. From then on, Zoom's Romanian subprocessor CSS Corp can exclusively process all Support Data within the EU. Only if admins urgently need support outside of regular EU working hours, they can consent to the use of TaskUS as a subprocessor in either the United States or the Philippines, according to a *follow-the-sun* model.

For this DPIA it is relevant whether customers have meaningful control over the engagement of subprocessors by Zoom and the processing of their personal data by such subprocessors. In dialogue

[110] Zoom new DPA, Clause 7.2.

[111] Idem, Clause 5.4.

[112] Idem, Clause 5.6.

with Zoom, SURF has obtained adequate guarantees about Zoom's control over its subprocessors, and has verified that no personal data is shared via Zoom's subprocessors to sub-subprocessors. The only exception to this rule could occur when organisations ignore the recommendations in this report, and use optional services such as Twilio to send invitations for Webinars. This DPIA has not examined additional risks of the use of such tools.

6.3. Data controller

As explained in Section 5.2.2 (Purposes Zoom as a data controller), Zoom is authorised to process some personal data for six purposes, as an independent data controller.

In abbreviated format, the six purposes are:

1. billing, account, and customer relationship management
2. complying with, and resolving legal obligations (including CSAM scanning)
3. abuse and virus detection, prevention, and protection
4. Using pseudonymised and/or aggregated data to improve and optimize the performance and core functionality of the Services
5. Using pseudonymised and/or aggregated data for internal (financial) reporting and planning
6. Using pseudonymised and/or aggregated data from Feedback for Zoom's overall service improvement

To some extent each service provider (that generally processes personal data as a data processor) is also a data controller for the use of some personal data about its customers. Each business needs to process some personal data to conduct limited and legitimate business operations, such as sending invoices.

Without prejudice to the assessment of the legal grounds and compliance with purpose limitation in Sections 12 and 13 of this DPIA, it is plausible that Zoom as an independent data controller can legitimately process some (limited) personal data for its own business purposes, when the processing is necessary. For example, when Zoom uses the limited set of Account Holder Data to send unsolicited commercial communications. Similarly, Zoom can legitimately act as an independent data controller for the personal data it collects from visitors to its publicly accessible website.

Zoom can use the Support Data for internal auditing of the effectivity of the support process. Zoom likely has a necessity and legitimate business interest to create statistics on the number of Accounts and revenues, volume and nature of network traffic and website visits for financial reporting and forecasting.

The processing of identifiable data for the first and third purpose is clearly necessary for Zoom as a company to run its business. The processing of pseudonymised or aggregated data (never on a per-Customer level) for the last three purposes is equally necessary for Zoom's legitimate financial and technical business operations. The processing for the second purpose, compliance with legal obligations, is discussed separately below, in Section 6.3.1.

Following the strict distinction between a processor and a controller, Zoom would be prohibited to process personal data it obtained as a processor in a role as controller, since a processor may not independently decide on purposes of the processing. The solution to this dilemma was recently explained by the French supervisory authority CNIL. Controllers may authorise their processors to 'further' process some personal data on their own behalf.[113] Following this logic, Zoom is contractually authorised by its customers to 'further' process some personal data for these six purposes without violating its processor obligations, as explained in Section 6.2. If the organisations remain in control, and perform the compatibility test themselves, and provide the written authorisation, they do not risk factually being qualified as joint controllers.

University and government administrators can enable the functionality of Feedback. This tool allows end-users to rate the quality of a conference call at the end of a meeting. If they are not satisfied, they can answer more questions, and enter free text in an open text field. If they enable this functionality, they authorise Zoom to anonymise these inputs, and use it for its overall service improvement. This is discouraged, as it is nearly impossible for the admins to oversee the compatibility of further processing of possible personal data included in the open text fields.

6.3.1. Disclosure to law enforcement

Zoom may necessarily have to process some personal data as a data controller when it receives valid requests from law enforcement authorities/courts.

According to the GDPR, only data controllers may take decisions to hand over personal data to law enforcement.[114] Article 48 of the GDPR creates an exception to this rule, acknowledging that a data processor may sometimes be forced by a court or administrative authority in a third country, outside of the EU, to transfer or disclose personal data. That may only be recognised or enforceable if it is based on an international agreement such as a mutual legal assistance treaty. This exception is titled "*Transfers or disclosures not authorised by Union law*". This exception therefore does not change the main rule that only data controllers may take decisions to hand over personal data.

It follows from the Zoom DPA that Zoom will first assess if it is a legitimate order. "*If so, Zoom will attempt to redirect this third party to request those data directly from Customer. If compelled to disclose or provide access to any Customer Personal Data to law enforcement Zoom will promptly*

[113] CNIL, Sous-traitants : la réutilisation de données confiées par un responsable de traitement, 12 January 2022, URL: https://www.cnil.fr/fr/sous-traitants-la-reutilisation-de-donnees-confiees-par-un-responsable-de-traitement.

[114] See for example the controller-processor opinion WP 169 from the Article 29 Working Party, p. 11, about the SWIFT-case: "*The fact itself that somebody determines how personal data are processed may entail the qualification of data controller, even though this qualification arises outside the scope of a contractual relation or is explicitly excluded by a contract. A clear example of this was the SWIFT case, whereby this company took the decision to make available certain personal data - which were originally processed for commercial purposes on behalf of financial institutions - also for the purpose of the fight against terrorism financing, as requested by subpoenas issued by the U.S. Treasury.*"

notify Customer and provide a copy of the demand unless legally prohibited from doing so. For example, through a so-called gagging order." [115]

Zoom commits in the DPA to represent the reasonable interests of its customers (the actual controllers), when compelled to disclose without informing its customer. The DPA lists five relevant conditions for such disclosure with which Zoom must always comply.

1. *Zoom shall document a legal assessment of the extent to which: (i) Zoom is legally obliged to comply with the request or order; and (ii) Zoom is effectively prohibited from complying with its obligations in respect of the Controller under this Addendum.*
2. *Zoom shall only cooperate with the request or order if legally obliged to do so and, where possible, Zoom shall judicially object to the request or order or the prohibition to inform the Controller about this or to follow the instructions of the Controller.*
3. *Zoom shall not provide more Customer Personal Data than is strictly necessary for complying with the request or order.*
4. *If Zoom becomes aware of a situation where it has reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by Zoom, its Affiliates and Authorized Subprocessors, including any requirements to disclose personal data or measures authorizing access by public authorities, will prevent Zoom from fulfilling its obligations under this Addendum, Zoom will inform Customer without undue delay after Zoom becomes aware of such a situation.*
5. *Zoom will publish a transparency report twice a year, documenting the amounts of received valid US nondisclosure orders and the number of orders complied with.*[116]

The fourth condition mirrors Clause 5 from the SCC that obliges Zoom as data importer to promptly notify the data exporter about any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation.

In its public information about its policy to deal with lawful requests from international authorities (outside of the USA) Zoom explains: "*We screen each international (non-U.S.) request carefully to ensure that we only respond to ones that are legally valid and appropriately scoped. We do not provide any content internationally without process under MLAT, the CLOUD Act or letters rogatory. If a jurisdiction or type of request is not listed in the chart's drop-down menus, it means we did not process any requests of that type or from that jurisdiction in this reporting period.*"[117]

---

[115] Zoom DPA, Clause 9.2.

[116] Zoom new DPA, Clause 9.2.

[117] Zoom's second Transparency Report, August 2021. Similarly, in its FAQs after the Schrems II-ruling, Zoom writes: "*Zoom's legal team reviews all government requests for data and will only disclose such data if legally compelled to do so (other than in emergency situations) and then, only in accordance with the applicable legal process. If a request is vague or overly broad, Zoom will challenge it.*" Zoom, FAQs: International Data Transfers, URL: https://explore.zoom.us/docs/doc/EEA_Transfer_of_Data.pdf.

Zoom has recently published a blog about these commitments. Zoom also explains in the blog that it participates in a lobby with other companies and NGOs to reform US surveillance laws. "*Zoom advances a thoughtful, balanced approach to governments' use of technology by participating in or consulting with organizations such as Reform Government Surveillance, the Center for Democracy and Technology and the Global Network Initiative, among others*." [118]

Based on the Schrems-II ruling, a recent expert legal analysis for the Dutch government, the analysis made by US law professor Stephen I. Vladeck (for the conference of the German State DPAs[119]), the report from Ian Brown and Douwe Korff about the future of data transfers to the USA for the LIBE committee of the European Parliament[120] and input provided to SLM Rijk and SURF by multiple cloud providers in 2021, an overview was created in Table 4 below of US laws that may be applied to compel US cloud services providers to disclose personal data from EU Enterprise and Education customers.

Zoom qualifies as an electronic communications service provider as defined in Title 50 of the United States Code (USC) § 1881(b)(4). The definition is as follows.

> The term "electronic communication service provider" means—
>
> a) a telecommunications carrier, as that term is defined in section 153 of title 47;
>
> b) a provider of electronic communication service, as that term is defined in section 2510 of title 18;
>
> c) a provider of a remote computing service, as that term is defined in section 2711 of title 18;
>
> d) any other communication service provider who has access to wire or electronic communications either as such communications are transmitted or as such communications are stored; or
>
> e) an officer, employee, or agent of an entity described in subparagraph (A), (B), (C), or (D).[121]

This means Zoom may be subjected to orders to hand-over personal data under FISA 702. Zoom is legally prohibited from disclosing such orders.

[118] Zoom, Government Requests and Data Protection, 18 January 2022, URL: https://blog.zoom.us/government-requests-and-data-protection/.

[119] Prof. Stephen I. Vladeck, Expert Opinion on the Current State of U.S. Surveillance Law and Authorities, 15 November 2021, URL: https://www.datenschutzkonferenz-online.de/media/weitere_dokumente/Vladek_Rechtsgutachten_DSK_en.pdf. Professor Vladeck previously acted as expert (together with Peter Swire) on behalf of Facebook in the Schrems-II case at the European Court of Justice, where he defended US intelligence gathering as offering 'essentially equivalent' protections, similar to the essential data protection guarantees in the EU. See for a summary of his points, IAPP, Understanding 'Schrems 2.0', URL: https://iapp.org/news/a/understanding-schrems-2-0/.

[120] Ian Brown and Douwe Korff, Study for the LIBE committee, Exchanges of Personal Data After the Schrems II Judgment, July 2021, URL: https://www.europarl.europa.eu/RegData/etudes/STUD/2021/694678/IPOL_STU(2021)694678_EN.pdf.

[121] See the official law website of the US government: https://uscode.house.gov/.

This table assumes Zoom also qualifies as "remote computing services" or "electronic communication services" (applicability of US Stored Communications Act and US CLOUD Act).[122] This table does not include legal obligations related to other US companies in other industries, such as banks or telecommunications carriers.

Table 4: Overview of US law that can be used to obtain personal data from EU Customers

US law enforcement and court orders	Type of authority, type of data	**US secret services surveillance**	Type of authority, type of data
Non-Disclosure orders can be issued up to one year[123] and have become 'commonplace'.[124] No principled restrictions on transparency reporting		Non-disclosure orders or general secrecy requirements. Transparency reporting is only permitted in ranges.[125]	
US Stored Communications Act, also allows for preservation orders for specific records/evidence[126]	Content Data: warrant signed by a judge. Requires *probable cause*.	Executive Order of the President (E.O.) 12333 as amended (limited) by Presidential Policy Directive (PPD) 28.[127] Since January 2021	Does not give direct authority to NSA to order cloud providers to hand-over data, but allows for bulk
	Non-Content Account Data (for example names and IP-addresses)[129]		

[122] "Remote Computing Service[s]" ("RCS") and "Electronic Communication Service[s]" ("ECS") are defined in 18 U.S.C. § 2510(15): *"'electronic communication service' means any service which provides to users thereof the ability to send or receive wire or electronic communications*"); and 18 U.S.C. § 2711(2) ("'*remote computing service' means the provision to the public of computer storage and processing services by means of an electronic communications system*").

[123] A judge can issue a protective order for all SCA and CLOUD Act orders "*when the independent judge determines that there is reason to believe that notification of the existence of the court order may create the adverse result of (1) endangering the life or physical safety of an individual; (2) flight from prosecution; (3) destruction of or tampering with evidence; (4) intimidation of potential witnesses; or (5) otherwise seriously jeopardizing an investigation or unduly delaying a trial.*" US Department of Justice, The purpose and impact of the CLOUD Act, Q&A 28, URL: https://www.justice.gov/dag/page/file/1153466/download The gagging orders are based on 18 U.S.C. § 2705. The maximum period of one year is mentioned in a memorandum from the Deputy Attorney General, 19 October 2017, URL: https://www.justice.gov/criminal-ccips/page/file/1005791/download.

[124] According to testimony of Microsoft VP Tom Burt for the House Committee on the Judiciary, 30 June 2021, URL: https://blogs.microsoft.com/on-the-issues/2021/06/30/the-need-for-legislative-reform-on-secrecy-orders/. For Zoom, this happens in roughly 50% of U.S. requests for user information.

[125] The secrecy requirements are defined in 18 U.S.C. § 1874, but the USA Freedom Act of 2015 authorizes four different options for companies to publish numerical information about the NSLs and FISA orders they receive.

[126] Clause 2703(f) of the US Stored Communications Act.

[127] Presidential Policy Directive 28 does not authorize intelligence gathering. It imposes limitations on how signals intelligence is gathered through other authorized means when targeting non-U.S. persons (e.g., the why, whether when and how the intelligence community targets foreign communications). Those means are articulated in the FISA 702 legal framework.

[129] The full list of 'Basic Subscriber Information' is defined in Title 18 of the United States Code (about Crimes and Criminal Procedure), U.S.C 2703(c)(2), *Required disclosure of customer communications or records*.

US law enforcement and court orders	Type of authority, type of data	**US secret services surveillance**	Type of authority, type of data
	subpoena from court, prosecutor or agency (judge not required)	Specified in NSA SIGINT Annex[128]	interception of transatlantic cables
	Other Non-Content (for example device information)[130]: court order or search warrant signed by a judge, lower standard of proof than for Content Data		
	Emergency requests: voluntary hand-over by providers (in case of imminent danger/death/serious physical injury)[131]		
US CLOUD Act (Clarifying Lawful Overseas Use of Data Act)	Expands the scope of the US Stored Communications Act to data stored outside of the EU, same authority requirements as above	Foreign Intelligence Surveillance Act (FISA) Section 702, limited to queries about non-U.S. persons located abroad. Section 702 no longer allows for the use of keywords. Sunset of FISA	Annual authorisation by the FISA Court (FISC).[132] FISC has authorized the collection of both metadata and content of communications

[128] NSA Sigint Annex, Procedures governing the conduct of DoD intelligence activities: Annex governing signals intelligence information and data collected pursuant to section 1.7(c) of E.O. 12333, URL: https://assets.documentcloud.org/documents/20454757/redacted-annex-dodm-524001-a.pdf .

[130] 18 USC 2703(c)(1) and 18 U.S.C. 2703(d), Record[s] or other information pertaining to a subscriber to or customer of such service.

[131] 18 U.S.C. 2702(c)(4).

[132] According to the U.S. Department of Commerce most U.S. organizations do not handle data that U.S. intelligence agencies are interested in and therefore do not engage in data transfers that present the type of privacy risks that appear to concern the ECJ. The Annual Statistical Transparency Report for 2020, published by the Office of the Director National Intelligence identifies the following number of Section 702 court orders: 1 in 2018, 2 in 2019 and 1 in 2020, and notes the following estimated number of targets relating to such orders as 164,770 for 2018, 204,968 for 2019 and 202,723 for 2020. Published April 2021, URL: https://www.dni.gov/index.php/newsroom/reports-publications/reports-publications-2021/item/2210-statistical-transparency-report-regarding-national-security-authorities-calendar-year-2020.

US law enforcement and court orders	Type of authority, type of data	**US secret services surveillance**	Type of authority, type of data
		Section 702 by the end of 2023	
Electronic Communications Privacy Act (ECPA), created amendments on the Stored Communications Act and the Wiretap Act and created the Pen Register Act.	Information relating to subscribers of "*wire or electronic communication service providers*."[133] Signed by a judge or customer notice of such requests	National Security Letters (FBI) based on ECPA	No prior approval from a judge, when relevant to authorized national security investigations. Can only order access to basic subscriber information, no content or Diagnostic Data.
Administrative subpoenas or demands (335 U.S. federal agencies)*	Based on the SCA, subject to the requirements described above	Title 1 (traditional) FISA warrant type a: existing account and metadata of U.S. Persons[134]	Applications to be approved by FISC
Search warrants to search and confiscate evidence, signed by judges based on state or local criminal laws (at least 57 distinct sets of laws[135])*	Based on the SCA, subject to the requirements described above	FISA warrant b: future metadata & content (tap) of U.S. Persons.	Applications to be approved by FISC
Judicially issued subpoenas and Grand Jury subpoenas for EU individuals to appear before a US court*	Based on the SCA, subject to the requirements described above	FISA business records order (Section 501, scope limited since 2020, no more 'any tangible	Applications to be approved by FISC

[133] 18 U.S.C. 2709, et seq.

[134] US Congressional Research Service, Foreign Intelligence Surveillance Act (FISA): An Overview, 6 April 2021, URL: https://crsreports.congress.gov/product/pdf/IF/IF11451. *Applications for 'regular' FISA warrants must include the following: (1) the applicant's identity; (2) information regarding the target's identity if known; (3) why the target may be searched or surveilled; (4) a statement establishing a sufficient relationship between the target and the search location; (5) a description of what will be searched or surveilled; (6) a description of the nature of the information sought or of the foreign intelligence sought; (7) proposed minimization procedures; (8) a discussion of how the search or surveillance will be carried out; and (9) a discussion of prior applications. If electronic surveillance is sought, applications must also discuss the duration of the surveillance. Traditional FISA warrants are issued for US persons, but may lead to the incidental data collection of non-U.S. persons when the U.S. person is the target of the FISA collection because they are suspected to be "a foreign power" or "an agent of a foreign power."*

[135] As mentioned by Professor Vladeck in his expert paper for the German DPAs, p. 10.

US law enforcement and court orders	Type of authority, type of data	US secret services surveillance	Type of authority, type of data
		thing'), for non-Content Data (Diagnostic Data)	
Incoming Mutual Legal Assistance requests filed by EU law enforcement to US Department of Justice Office of the International Affairs		FISA pen registers and trap and trace devices (as expanded by US Patriot ACT from 2015 to internet communications)[136]	Applications to be approved by FISC, no probable cause required

* Some of these law enforcement powers may not apply to data stored outside the United States, both in general and because of the strong presumption U.S. courts apply against the extraterritorial application of statutes.[137]

Zoom transparency reporting

In order to assess the likelihood of the risk for data subjects that their data are subjected to inspection by foreign LEAs or Security Services, transparency from Zoom is important. On 18 December 2020, Zoom published its first semi-annual Transparency report. [138] In August 2021, Zoom published its second Transparency report. In February 2022, Zoom published its third Transparency report.[139]

In its Transparency reports Zoom publishes statistics about enforcement requests from US authorities, and requests from the authorities in the rest of the world, including the EU. Zoom does not distinguish between consumer accounts and Education/Enterprise accounts. Zoom also does not distinguish between users in the USA and users outside of the USA.

In dialogue with SURF, Zoom explained the context of the requests it receives. Zoom gave the following fictive example.

Fictive example of US law enforcement request

"A US University hosted a Zoom event called "Tackling the Climate Emergency: How U.S. and E.U. Companies Can Lead the Way". 57 people attended. Some were logged into Enterprise and Education Zoom accounts (both EU and US). Some had Zoom pro accounts, some had basic accounts (which do not have physical addresses) and some attended via browser. When users join from a browser, they select their own screen names and don't have to give any real information about themselves. 12 minutes into the meeting, some of the attendees started displaying child sexual abuse material,

[136] Applications do not require the identity of a suspect, only (1) the identity of the federal officer seeking to use a PR/TT device; (2) the applicant's certification that the information likely to be obtained is foreign intelligence information; and (3) a specific selection term to be used as the basis of the PR/TT device.

[137] As mentioned by Professor Vladeck, with a reference to Supreme Court jurisprudence from 2016, RJR Nabisco, Inc. v. European Community, 136 S. Ct. 2090, 2099–100 (2016).

[138] Zoom first transparency report, URL: https://explore.zoom.us/docs/en-us/transparency.html.

[139] Zoom second and third transparency report, URL: https://explore.zoom.us/docs/en-us/trust/transparency.html.

drawing swastikas on the white board, shouting over the speaker, renaming themselves and playing loud music. The host ended the meeting and reported the event to the university police. The university police served Zoom with a subpoena asking for the BSI of everyone in the meeting to try to figure out who displayed the swastika and the CSAM. Zoom's Law Enforcement Response Team pulled the attendee list. First it eliminated all attendees who didn't share their screens or use audio or video. Then Zoom gave the university policy the BSI for everyone else."

With this example, Zoom also explained why it cannot accurately make the distinction between US and EU customers, because it often doesn't know where its users are located.[140] If Zoom, in another example, receives a subpoena from the FBI for the Account Data (Basic Subscriber Information, includes name, e-mail address and IP address), relating to a particular meeting organised by a US cryptocurrency company suspected of wire fraud, and a user with an EU Education account participated in that meeting, Zoom may disclose the Account Data of that end user to the FBI without knowingly providing data about EU customers. Zoom mentioned two more reasons why it cannot reliably know the location of its users.

1. Zoom sees only limited information of participants that joined via their browser, because they do not have to give any real information about themselves. Zoom only sees their IP addresses, but cannot see if the user is a consumer or a member of an Education or Enterprise account.

2. Users can use a VPN. Their IP address then seems to originate from a different location. Zoom cannot tell if an IP address is issued by VPNs or represent the user's actual location.

Therefore, Zoom's statistics do not provide EU Education and Enterprise customers with exact numbers to estimate the chance that their specific data are requested by US government authorities. However, close reading of Zoom's transparency reporting seems to reveal that it has not yet received any FISA Section 702, National Security Letters or US Cloud Act requests, since these specific orders are not mentioned in its statistics.

As Zoom explains in its reports*:"If a jurisdiction or type of request is not listed in the chart's drop-down menus, it means we did not process any requests of that type or from that jurisdiction in this reporting period."*[141]

[140] Response Zoom to SURF, 28 January 2022.

[141] Zoom second and third transparency report, URL: https://explore.zoom.us/docs/en-us/trust/transparency.html.

Figure 19: Zoom overview of US requests for all of its customers, May-December 2020[142]

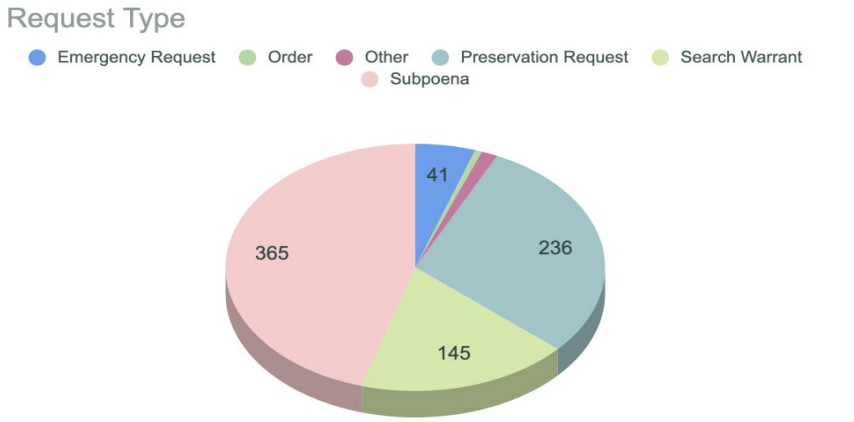


Figure 20: Zoom statistics about resolution of US requests, May – December 2020[143]

	Resolution				
About	General Information	Non-content	Preservation Fulfilled	Rejected	Grand Total
Emergency Request	1	26		14	41
Order		5			5
Other		5		6	11
Preservation Request	1	1	201	33	236
Search Warrant	1	111		33	145
Subpoena		274		91	365
Grand Total	**3**	**422**	**201**	**177**	**803**

[142] Zoom first transparency report, URL: https://explore.zoom.us/docs/en-us/transparency.html.

[143] Idem.

Figure 21: Zoom overview of US requests for all of its customers, January-June 2021[144]

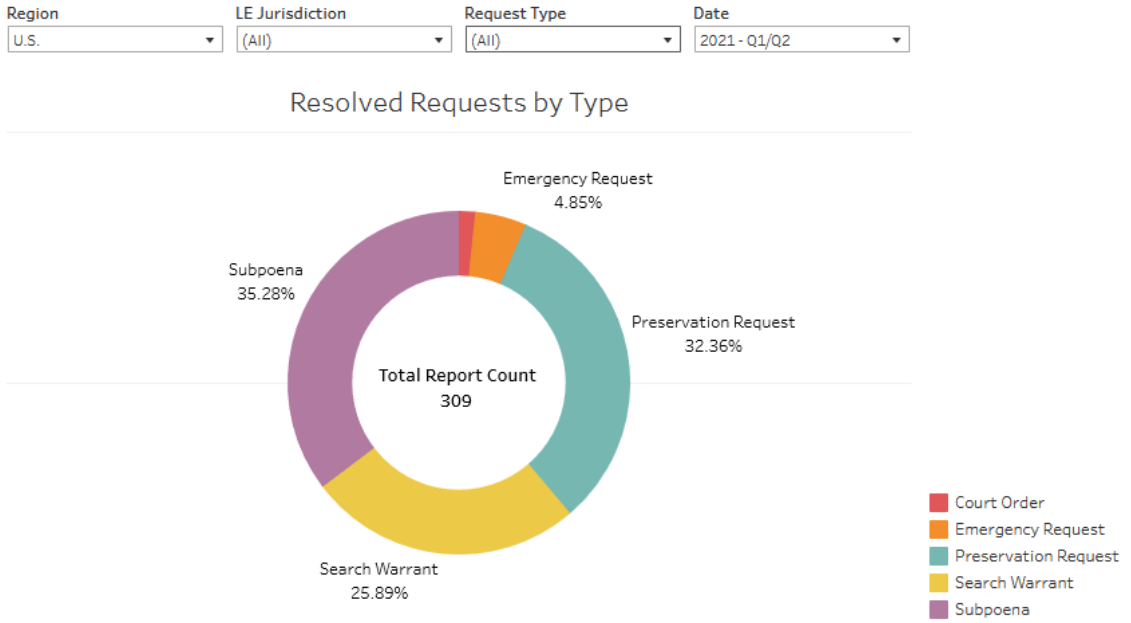
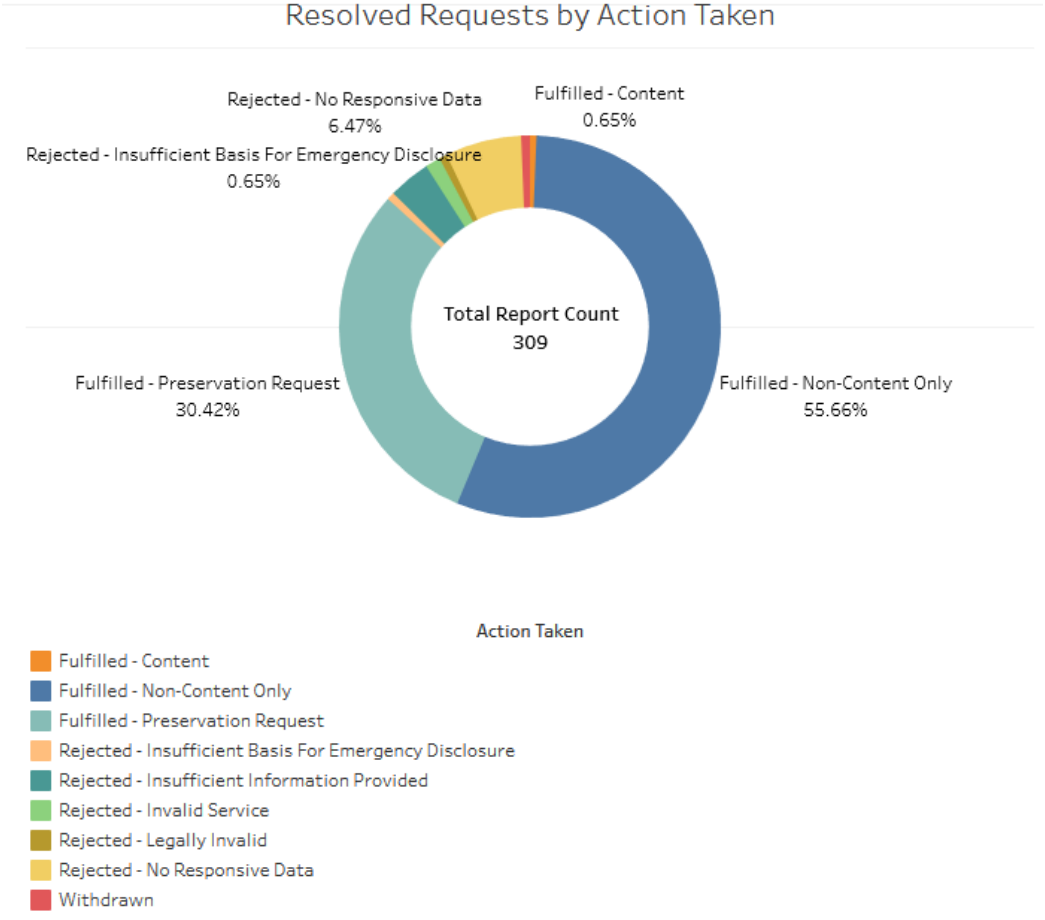


Figure 22: Zoom statistics about resolution of requests, January-June 2021



[144] Zoom second transparency report, URL: https://explore.zoom.us/docs/en-us/trust/transparency.html

7. Interests in the data processing

This section outlines the different interests of Zoom and Dutch universities and government organisations in the use of Zoom Meetings. The interests of the Dutch government organisations may align with the interests of their employees, but this is not always the case. This section does not include an analysis of the fundamental data protection rights and interests of employees as data subjects. How their rights relate to the interests of Zoom and the Dutch universities and government organisations is analysed in part B of this DPIA.

7.1. Interests universities and government organisations

Dutch universities and government organisations have security, efficiency and compliance reasons to use (paid) videoconferencing services such as Zoom Meetings Enterprise.

A key data protection and security benefit of the use of the Education/Enterprise version, compared to the Basic (free) version is the availability of administrator controls to limit the data processing.

Zoom Meetings is able to provide end-to-end-encryption of the transmission of streaming audio and video data between participants, also for 'basic' (free) Zoom accounts, and hence, also for guest users. This provides protection against bulk surveillance and interception of the communication. As will be explained in Section 9.1 of this report, the chat functionality can also be encrypted with keys controlled by the participants on their own devices.

Additionally, the ability to access log data about end user behaviour through the different audit logs in the admin Console, with Zoom's commitment to provide an easier take-out per end-user, as well as a take-out for admin behaviour, is essential for government organisations to comply with their own obligations as data controllers to detect security incidents and data breaches.

With Zoom Meetings Enterprise, an organisation can determine its own data protection and security policy, select the appropriate central settings, and thus use the services to meet its security and data protection compliance needs. If the Dutch universities and government organisations do not sign-up for an Education or Enterprise contract, there is a risk that employees share information via consumer versions of the Zoom services, or through other 'free' tools. Such work information may be sensitive or confidential and can be shared with participants outside of the work environment. If the exchange happens between consumer applications, the administrator cannot enforce the organisation's data protection and security policy, nor detect such data breaches via the operator log files.

Dutch universities and government organisations already have the possibility to use a centrally negotiated Education and Enterprise version of Microsoft Teams for conference calling. But for security reasons, it is better to spread the risks of outages or single points of failures by contracting with different providers of videoconferencing tools and services. Additionally, Zoom offers E2EE for all meetings, where Microsoft currently only offers E2EE for unscheduled 1-on-1 calls.

All organisations have a strong interest in providing reliable, always working, well integrated and location independent communication tools to their employees. Well-functioning also means that the

software has to be accessible on different kinds of devices, and from different locations. The ability for employees and students to seamlessly work at home and collaborate with each other through videoconferencing tools, remains as urgent as ever since the outbreak of the COVID-19 pandemic.

In contrast with the above-mentioned interests in the use of a cloud provider such as Zoom, organisations must continue to comply with the GDPR, as explained by the EDPB. In view of the strict EDPB guidance on the transfer of personal data to the USA, all organisations in the EU should at least inventory the possibility to use alternative services or *on-premise* software that are not controlled by a US mother or subsidiary. Even though Zoom offers E2EE for the streaming content, there is no such guarantee for the data about the use of its services. This balancing exercise is further explained in Section 8.

7.2. Interests of Zoom

Zoom has a strong financial and economic interest in upselling customers of its free Basic services to a paid Enterprise subscription service in order to generate revenue.

Zoom is a publicly held company since 18 April 2019 and has published two annual financial reports a Form 10-K for the fiscal years ending 31 January 2020 and 31 January 2021.[145] In these forms Zoom describes that its net cash already tripled from 51 to 152 million US dollars at the end of 2019. In 2020, Zoom's user base skyrocketed. Zoom went from 10 million users at the end of 2019, to 300 million in April 2020, during the global outbreak of the COVID-19 pandemic. Counting both free and paying users, in July 2021 Zoom had 300 million daily meeting participants.[146]

At the end of January 2021, Zoom's revenue had increased to $2,651.4 million US dollars, a growth rate of 326% compared to the 622,7 million US dollars revenue at the start of 2020. An increasing share of this revenue comes from outside of the US (APAC and EMEA), from 18% in the year ending January 2019, to 19% at the start of 2020 to 31% at the start of 2021.[147]

In its financial report over 2020, Zoom separately describes the exponential growth in the amount of paying Education/Enterprise customers: *"As of January 31, 2021, 2020, and 2019, we had approximately 467,100, 81,900, and 50,800 customers, respectively, with more than 10 employees."*[148]

For its business growth, Zoom relies on word of mouth via viral marketing, and on upselling of its existing customers. "*We have a unique model that combines viral enthusiasm for our platform with a multipronged go-to-market strategy for optimal efficiency. Viral enthusiasm begins with our users as they experience our platform – it just works. This enthusiasm continues as meeting participants become paid hosts and as businesses of all sizes become our customers. Our sales efforts funnel this*

[145] Zoom Forms 10-K filed for the United States Securities and Exchange Commission, URL: https://investors.zoom.us/sec-filings/?field_nir_sec_form_group_target_id%5B%5D=471&field_nir_sec_date_filed_value=&items_per_page=10#views-exposed-form-widget-sec-filings-table.

[146] Backlink, Zoom User Stats: How Many People Use Zoom in 2022? 6 January 2022, URL: https://backlinko.com/zoom-users.

[147] Zoom Form 10-K for the year ending 31 January 2021, p. 22.

[148] Idem, p. 47.

viral demand into routes-to-market that are optimized for each customer opportunity, which can include our direct sales force, online channel, resellers, and strategic partners."[149]

Zoom also writes: "*Our business depends on our ability to attract new customers and hosts, retain and upsell additional products to existing customers, and upgrade free hosts to our paid offerings. Any decline in new customers and hosts, renewals, or upgrades would harm our business*." [150]

In reply to DPIA questions Zoom has emphasised that it is "not a social media or "big data" company. "*We do not sell or monetize customer meeting data. Our primary product has always been the provision of internet video conferencing services to corporate customers in exchange for subscription fees (rather than user data).*"[151]

Zoom's mission is to make video communications frictionless and secure. Zoom dedicates many paragraphs in its annual financial report to the risks of non-compliance with privacy and security requirements such as the GDPR. In its second annual report, Zoom writes about risks and liabilities related to the transfer of personal data from the EU to the US, and already anticipates on its new commitment to build an exclusive EU cloud:

"*If we are unable to implement a valid solution for personal information transfers from Europe, we will face increased exposure to regulatory actions, substantial fines, and injunctions against processing or transferring personal information from Europe, and we may be required to increase our data processing capabilities in Europe at significant expense. Inability to import personal information from Europe to the United States or other countries may decrease demand for our products and services as our customers that are subject to the GDPR may seek alternatives that do not involve personal information transfers out of Europe. Our inability to import personal information to the United States and other countries may decrease the functionality or effectiveness of our products and services and adversely impact our marketing efforts, plans and activities. We expect EU regulators to aggressively enforce EU laws prohibiting data transfers to the U.S. and other countries without a legally sound transfer mechanism, and it possible that EU regulators could prevent Zoom from transferring any personal data out of the EU to certain countries like the U.S.*"[152]

Zoom has business and economic interests to compete with competitors such as Microsoft, Cisco, and Google. Zoom writes:

"*The market for communication and collaboration technologies platforms is competitive and rapidly changing. Certain features of our current platform compete in the communication and collaboration technologies market with products offered by:*

- *legacy web-based meeting providers, including Cisco WebEx and LogMeIn GoToMeeting;*
- *bundled productivity solutions providers with video functionality, including Microsoft Teams and Google G Suite and Meet products;*
- *UCaaS and legacy PBX providers, including Avaya, RingCentral, and 8x8; and*

[149] Idem, p. 6.

[150] Idem, p. 4.

[151] Zoom Answers to DPIA questions, 23 November 2020, Introduction.

[152] Zoom Form 10-K for the year ending 31 January 2021, p. 29.

- *consumer-facing platforms that can support small- or medium-sized businesses, including Amazon, Apple and Facebook."*[153]

Zoom explained that it focuses on privacy and security now that it has grown so rapidly: "*The Covid pandemic brought about significant change to our business, which has led to us making a huge investment in data protection and information security. Our user base grew and diversified significantly. For context, we grew from 10 million daily meeting participants as of December 2019, to over 300 million a day in April 2020, including new clients in schools and universities.*"[154]

Zoom also has a direct monetary incentive in providing and enforcing compliance with security guarantees. In the spring of 2020, Zoom generated a lot of negative publicity about privacy and security breaches, including incidents like falsely claiming effective end-to-end encryption, sharing data from the iOS app with Facebook, a now disabled function for attendee attention tracking, and the widely reported access to meetings by uninvited guests (*Zoom bombing*).[155] In November 2020, Zoom reached a settlement with the Federal Trade Commission in the USA that requires Zoom to implement a robust information security program. The so called 'Consent Order' puts Zoom for the next 20 years under heightened scrutiny of the supervisory authority. If Zoom violated any of the agreed terms of the Order, it would become liable for civil penalties and other relief.

The order explicitly "*prohibits Zoom from making misrepresentations about its privacy and security practices, including about how it collects, uses, maintains, or discloses personal information; its security features; and the extent to which users can control the privacy or security of their personal information.*"[156]

This however does not equal an obligation to provide full and accurate data protection information, as FTC Commissioner Slaughter notes in her dissenting opinion on the Consent Order.[157]

Slaughter opines: "*When Zoom's user base rapidly expanded, its failure to prioritize privacy and security suddenly posed a much more serious risk in terms of scope and scale. This proposed settlement, however, requires Zoom only to establish procedures designed to protect user security and fails to impose any requirements directly protecting user privacy.*"[158]

7.3. Joint interests

The interests of Zoom and the universities and government organisations align when it comes to protecting the personal data against unauthorised access with strong security measures. This includes

[153] Idem, p. 9.

[154] Zoom Answers to DPIA questions, 23 November 2020, Introduction.

[155] See for example the EFF overview of the issues with Zoom at https://www.eff.org/deeplinks/2020/03/what-you-should-know-about-online-tools-during-covid-19-crisis.

[156] FTC and Zoom Consent Order, 9 November 2020, URL: https://www.ftc.gov/system/files/documents/cases/1923167zoomacco2.pdf.

[157] FTC, dissenting statement of commissioner Rebecca Kelly Slaughter In the Matter of Zoom Video Communications, Inc., Commission File No. 1923167, 9 November 2020, URL: https://www.ftc.gov/system/files/documents/public_statements/1582918/1923167zoomslaughterstatement.pdf.

[158] Idem.

the use of multi factor authentication and effective end-to-end encryption. Zoom and its Education and Enterprise customers have a joint interest in the processing of some personal data, when necessary, to provide a secure, well-functioning and bug free service, which responds to the settings from each customer, and to provide support. Through the new Zoom DPA, organisations can authorise Zoom to process personal data for these purposes in a role as processor, when such processing is necessary.

Zoom's commitment to develop exclusive EU data processing by the end of 2022 ensures that the personal data from EU customers are protected against direct surveillance in the USA. Though this does not by itself mitigate all risks of undue government access to the personal data, it greatly helps mitigating the data protection risks for the data subjects in the EU.

There will be one exception to the EU data processing rule: Zoom's continued transfer of pseudonymous and aggregated Diagnostic Data to its central Trust & Safety team in the USA. Organisations have a joint interest with Zoom in enabling Zoom to centrally detect and mitigate security incidents, based on input from its global customer base. Thanks to its scale and centralised operations, it is plausible that Zoom is better equipped than local alternative solutions to secure the streaming or stored Content Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access. Though the DTIA performed for this transfer shows that this transfer poses a low risk for data subjects, it is possible that the EDPB will rule such systematic transfers unlawful. In that case Zoom and its customers have a mutual interest in finding an effective solution. As noted in Section 7.1, pending further EDPB guidance, Dutch universities and government organisations should at least inventory the possibility to use alternative services or *on-premise* software that are not controlled by a US mother or subsidiary.

8. Transfer of personal data outside of the EEA

8.1. Zoom's factual transfers of personal data

Until Zoom has completed its EU Cloud (by the end of 2022) Zoom systematically transfers personal data from its EU customers to the USA.

Zoom uses a mix of cloud technologies and its own colocated data centres to deliver its services. Prior to the Covid-19 pandemic, real-time traffic for paying customers was routed primarily through Zoom's colocated data centres, with capacity backup from Amazon Web Services (AWS), and AWS hosted pre-meeting and post-meeting data. Since the pandemic struck, a large quantity of real-time video-conferencing traffic has moved to AWS and a much smaller amount of capacity has moved to the Oracle Cloud.

Zoom's colocation facilities are provided by Digital Realty, Level 3, CoreSite, Aptum, Equinix, Tata, Telstra, Telx, and Zayo.

Zoom offers two types of geolocation choices to its Enterprise and Education users: for the routing of data exchanged during meetings, and for a subset of stored data (data-at-rest).

Since the end of January 2021, Zoom offers a geolocation choice to its paying customers to store a limited subset of the Content Data in data centres in the EU.

Zoom explains: *"[Since the end of January 2021] Zoom Customers with a Pro, Business/Enterprise, and Education license can designate certain storage locations for their meeting recordings, meeting transcripts, in-meeting chat messages, and files exchanged during a meeting.*

[However] Persistent chat messages (for users of Zoom's out-of-meeting chat feature), Account Data, and operation data will continue to be stored in the default storage location of the US.

Account administrators for paying Zoom customers can select one of the following regions to exclusively store certain (Customer) Content Data (cloud recordings, meeting transcripts, in-meeting chat messages, files exchanged in -meeting via chat):

- *United States*
- *Australia*
- *Brazil*
- *Canada*
- *Germany*
- *Japan*
- *Singapore*" [159]

However, this geolocation choice only applies to a limited set of personal data, the Content Data, with the exception of back-ups. Zoom explains that backups are stored in the US by default: "*Backups are stored by default in the US. In certain cases, a customer account may be mitigated to our Canadian or EU cluster, in which case, backups of Communications Content (recordings and transcripts) will be stored in the migration destination*." In other words, when a Customer account is provisioned to an EU server, as will be the case with the SURF accounts, backups will also be stored in the EU.

As show in Figure 16 in Section 4.2.2, Education and Enterprise customers can choose data center regions (plus the automatically determined home region) for the hosting of their real-time meeting and webinar traffic. Customers may also choose to store recordings locally, on their own devices/in their local data centre.[160]

Zoom has confirmed in reply to this Update DPIA that it technically redirects its European visitors to the EU-hosted restricted access pages. If Zoom's EU customers use a Vanity URL, this traffic will also automatically be hosted in the EU instances of AWS.

Zoom does not yet offer the possibility to administrators to exclusively process any other personal data in the EU. The Account, Diagnostic, Support and public Website Data are directly transferred or generated on Zoom's servers in the USA. By mid-2022, EU customers will be able to select EU-only for their support requests.

[159] Zoom reply to part A of the DPIA, 19 March 2021, p. 13.

[160] Zoom, Protecting your data, URL: https://zoom.us/trust/security.

Zoom currently uses datacentres in 12 countries/territories.[161] The personal data can be routed via other locations during the transfer and can also be processed in other regions. Technically, the routing of packets via the Internet works in such a way that the paths (and therefore locations) that will be followed cannot be determined in advance. It is however possible to exclude regions. To this end, Zoom offers Controlled data routing. This allows Enterprise and Edu customers to opt in or out of a specific data center region for data in transit.[162]

8.2. GDPR rules for transfers of personal data

The GDPR contains specific rules for the transfer of personal data to countries outside the European Economic Area (EEA). In principle, personal data may only be transferred to countries outside the EEA if the country has an adequate level of protection. That level can be determined in several ways: a multinational may adopt Binding Corporate Rules, apply the EU Standard Contractual Clauses (SCC), or only transfer to countries for which the European Commission has taken a so-called adequacy decision. In case of incidental, unsystematic transfers, organisations may also look for a transfer legitimation in Article 49 of the GDPR. For Zoom this option is only available for some Website Data, if its website visitors provide active consent for the use of other than strictly necessary cookies and provide explicit consent for the ensuing transfer of personal data to the USA.

8.2.1. Standard Contractual Clauses

Personal data may be transferred from the EEA to third countries outside of the EEA using Standard Contractual Clauses (SCC, also known as EU model clauses) adopted by the European Commission.[163] These clauses (hereinafter: SCC) contractually ensure a high level of protection.

8.2.2. European Commission Adequacy decision

An adequacy decision means that the country in question has a level of protection comparable to that applied within the EEA. Currently, there are adequacy decisions with respect to Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Republic of Korea, Switzerland, the UK, and Uruguay.[164] The adequacy decision for (some transfers under the Privacy Shield to) the USA is no longer valid since the summer of 2020.

---

[161] Zoom, Selecting data center regions for hosted meetings and webinars, URL: https://support.zoom.us/hc/en-us/articles/360042411451-Selecting-data-center-regions-for-meetings-webinars.

[162] Idem. See also Zoom, Selecting data center regions for hosted meetings and webinars, URL: https://support.zoom.us/hc/en-us/articles/360042411451-Selecting-data-center-regions-for-hosted-meetings-and-webinars.

[163] Based on the Annex to the Commission Implementing Decision on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/6794 June 2021, URL: https://ec.europa.eu/info/system/files/1_en_annexe_acte_autonome_cp_part1_v5_0.pdf.

[164] European Commission, Adequacy decisions, URL last visited 28 January 2022: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.

8.2.3. Schrems-II ruling European Court of Justice: FISA Section 702 and E.O. 12333

On 16 July 2020, the European Court of Justice ruled that transfer of personal data based on the Privacy Shield was no longer valid, with immediate effect.[165] This judgment was the outcome of the lawsuit Max Schrems conducted against Facebook Ireland and the Irish Data Protection Commissioner. Earlier, in 2015, in another case instigated by Max Schrems, the European Court ruled the Safe Harbor agreement invalid, the predecessor of the Privacy Shield.

The Privacy Shield itself is since invalid as a legal basis for the transfer of personal data. The Court cited as the main reasons that the restrictions on privacy arising from the U.S. regulations are insufficiently defined and disproportionate and therefore constitute too great an invasion of privacy. Specifically, the Court describes the risks of mass surveillance (bulk data collection) by U.S. intelligence agencies under the surveillance programs PRISM and Upstream based on Section 702 FISA and based on E.O. 12333, and the lack of effective and enforceable rights for EU residents in the processing of those data by U.S. government agencies.

8.2.4. US Cloud Act and other applicable US law

In addition to these two specific surveillance powers, the USA legal regime enables law enforcement authorities and secret services to compel cloud providers to disclose personal data from their European customers, also when the data are stored in data centres in the EU. Table 4 in Section 6.3.1 contains all known US laws that can be applied to Zoom. As mentioned in Section 6.3.1, two US senators have recently revealed the existence of a CIA bulk surveillance system based on EOP 12333.[166]As it is (yet) unknown what categories of personal data are collected as part of this program (telecom, or other categories, relating to for example banking or travel), the table does not include these powers.

The US CLOUD Act (*Clarifying Lawful Overseas Use of Data*) was specifically designed to obtain access to data stored in data centres in the EU. This act extends the jurisdiction of North American courts to all data under the control of U.S. companies, even if those data are stored in data centres outside the territory of the United States.

As explained by the EDPB and the European Data Protection Supervisor (EDPS) in their opinion on the CLOUD Act to the LIBE Committee of the European Parliament, transfers of personal data from the EU must comply with the Articles 6 (lawfulness of processing) and 49 (derogations for specific situations) of the GDPR. In case of an order based on the US CLOUD Act, the disclosure and transfer can only be valid if recognised by an international agreement between the EU and the USA.

The EDPB and EDPS write: "*Unless a US CLOUD Act warrant is recognised or made enforceable on the basis of an international agreement, and therefore can be recognised as a legal obligation, as per*

[165] European Court of Justice, C-311/18, Data Protection Commissioner against Facebook Ireland Ltd and Maximillian Schrems (Schrems-II), 16 July 2020.

[166] New York Times, C.I.A. Is Collecting in Bulk Certain Data Affecting Americans, Senators Warn, 10 February 2022, URL: https://www.nytimes.com/2022/02/10/us/politics/cia-data-privacy.html. See also: the letter the senators wrote at: https://int.nyt.com/data/documenttools/haines-burns-wyden-heinrich-13-apr21-final/47ab462e38b8e5f7/full.pdf.

Article 6(1)(c) GDPR, the lawfulness of such processing cannot be ascertained, without prejudice to exceptional circumstances where processing is necessary in order to protect the vital interests of the data subject on the basis of Article 6(1)(d) read in conjunction with Article 49(1)(f)." [167]

In their cover letter, the data protection authorities emphasize "*the urgent need for a new generation of MLATs to be implemented, allowing for a much faster and secure processing of requests in practice. In order to provide a much better level of data protection, such updated MLATs should contain relevant and strong data protection safeguards such as, for example, guarantees based on the principles of proportionality and data minimisation.*" Additionally, the data protection authorities refer to the ongoing negotiations since 2019 about an international agreement between the EU and the US on cross-border access to electronic evidence for judicial cooperation in criminal matters and negotiating directives.[168]

Only the UK has so far signed a specific agreement with the USA for the Cloud Act. Negotiations between the EU and the US about updated MLATs, as well as negotiations about a successor for the Privacy Shield, did not produce any results yet.[169]

8.3. Data Transfer Impact Assessment (DTIA)

Zoom generally uses the (new 2021) SCC to legitimise the transfer of all personal data from its EU customers to the USA, or the Philippines (for customer support). "*Storage of operations and pre-and post-meeting activities, including storage of (Customer) Content, occur on AWS' servers which are located in Australia, Canada, China, India, Japan, the EU and the US. Zoom and AWS have concluded the Standard Contractual Clauses (SCCs) to protect the transfer of EEA/UK residents' data out of the EEA/UK.*"

When Zoom transfers data between its affiliates (group companies), Zoom relies on an intra-group data transfer agreement that applies the SCCs to help protect the privacy and security of EEA/UK residents' personal data."[170]

Although the European Court of Justice recognizes the validity of the decision of the European Commission with which it adopted the SCC, and data transfers on the basis of the SCC are therefore still permitted in principle, this validity cannot be assumed for systematic transfers of personal data to the United States.

---

[167] Annex EDPB and EDPS joint response to US CLOUD Act, 10 July 2019, p. 8. URL: https://edpb.europa.eu/our-work-tools/our-documents/letters/epdb-edps-joint-response-libe-committee-impact-us-cloud-act_en.

[168] Council Decision authorising the opening of negotiations, 6 June 2019, URL: https://data.consilium.europa.eu/doc/document/ST-10128-2019-INIT/en/pdf and https://data.consilium.europa.eu/doc/document/ST-10128-2019-ADD-1/en/pdf.

[169] See an update in US based news source Politico, Digital Bridge: Privacy Shield update 3.0 — Semiconductor subsidies — EU-US policy spat, 3 February 2022, URL: https://www.politico.eu/newsletter/digital-bridge/privacy-shield-update-3-0-semiconductor-subsidies-eu-us-policy-spat/.

[170] Zoom reply to part A of the DPIA, 19 March 2021, p. 13.

The fact is that transfers via the SCC also require that the recipient country provides an adequate level of data protection as defined in EU law. Article 46(1) of the General Data Protection Regulation (GDPR) explains that this means that data subjects must have adequate safeguards, enforceable rights and effective legal remedies at their disposal. Whether this is the case, according to the Court, must be determined by the data controllers and cloud providers themselves.

The Court writes: "*The assessment required for that purpose in the context of such a transfer must, in particular, take into consideration both the contractual clauses agreed between the controller or processor established in the European Union and the recipient of the transfer established in the third country concerned and, as regards any access by the public authorities of that third country to the personal data transferred, the relevant aspects of the legal system of that third country. As regards the latter, the factors to be taken into consideration in the context of Article 46 of that regulation correspond to those set out, in a non-exhaustive manner, in Article 45(2) of that regulation.*"[171]

The EDPB explains that there are four guarantees that make limitations to the data protection and privacy rights as recognised by the Charter justifiable.[172]

These four guarantees are:

1. Processing should be based on clear, precise, and accessible rules
2. Necessity and proportionality concerning the legitimate objectives pursued need to be demonstrated
3. An independent oversight mechanism should exist
4. Effective remedies need to be available to the individual

These criteria are essential guarantees, the EDPB adds, but not sufficient by itself to determine whether the legal regime of the third country offers an essentially equivalent level of protection.

It follows from the Schrems II ruling that the current legal regime in the USA, in particular the FISA Section 702 legislation, does not meet these four criteria, for the following reasons:

1. FISA Section 702 and E.O. 12333 do not indicate limitations on the powers they confer to implement surveillance programmes for the purposes of foreign intelligence.
2. US laws permit public authorities to have access on a generalised basis to the content of electronic communications. This must be regarded as compromising the essence of the fundamental right to respect for private life, as guaranteed by Article 7 of the Charter.
3. The scope of the supervisory role of the oversight mechanism by the US Ombudsman does not cover the individual surveillance measures. It is doubtful whether the US Ombudsman meets the other elements for independence defined by the European Court of Human Rights

[171] Idem, par 104.

[172] EDPB, Recommendations 02/2020 on the European Essential Guarantees for surveillance measures, Adopted on 10 November 2020, URL: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_recommendations_202002_europeanessentialguaranteessurveillance_en.pdf.

in its jurisprudence about surveillance measures, such as independence from the executive, being vested with sufficient powers and competence and whether its activities are open to public scrutiny.

4. Closely related to the third guarantee, data subjects from the EU whose data are transferred to the USA cannot bring legal action before an independent and impartial tribunal in order to have access to their personal data, or to obtain the rectification or erasure of such data.

Zoom publishes separate questions and answers about the transfer of personal data post-*Schrems II*.[173] In this document, Zoom confirms it qualifies as *communication service provider* as defined in 50 USC § 1881(b)(4).

"*Most, if not all, US-based providers of cloud-based technology solutions will fall within the scope of an "electronic communications service provider". Zoom is no different in this respect.*"[174]

This means Zoom may be subjected to orders to hand-over personal data under Executive Order 12333 and FISA 702. Providers are prohibited from informing their customers about such orders. As explained in Section 6.3.1 of this DPIA, Zoom has published three transparency reports about the number of requests it receives from law enforcement and secret services.

8.3.1. Analysis of the chances that the risk of undue access occurs

As part of this DPIA, a DTIA was performed. Such a DTIA is necessary to assess whether the SCCs offer an essentially equivalent protection to the transferred data to Zoom. The DTIA is attached in Excel. The analysis is based on the format created by the Swiss legal scholar David Rosenthal, with some additions.[175]

The definition of 'transfer' is not clear. The EDPB suggests that there is no transfer when a cloud provider can promise that all data are exclusively processed in the EU: "*Keep in mind that remote access from a third country (for example in support situations) and/or storage in a cloud situated outside the EEA offered by a service provider, is also considered to be a transfer. More specifically, if you are using an international cloud infrastructure you must assess if your data will be transferred to third countries and where, unless the cloud provider is established in the EEA, and it clearly states in its contract that the data will not be processed at all in third countries.*"[176]

In a footnote in its guidance on supplementary measures in case of transfer, the EDPB suggests that any access from a third country counts as a transfer: "*Please note that remote access by an entity from a third country to data located in the EEA is also considered a transfer*."[177] This DPIA assumes that the

[173] Zoom, FAQS: Transferring EEA & UK Residents' Data to the US. Zoom refers to these FAQs in its Answers to DPIA questions from 23 November 2020.

[174] Idem.

[175] David Rosenthal, EU SCC Transfer Impact Assessment (TIA) Toolbox, with templates/samples for the various jurisdictions and a questionnaire for assessing foreign lawful access laws, published under free Creative Commons "Attribution-ShareAlike 4.0 International" (CC BY-SA 4.0) license, URL: https://www.rosenthal.ch/downloads/Rosenthal_EU-SCC-TIA.xlsx.

[176] EDPB, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, Version 2.0, Adopted on 18 June 2021, Par. 13, p. 11.

[177] Idem, footnote 23.

term transfer includes (the possibility) of orders from US government authorities to disclose personal data for EU customers, hence the need for a Data Transfer Impact Assessment, even for the streaming Content Data in Zoom Meetings, that are already processed in the EU.

The EDPB describes different elements of the risk assessment in its guidance on *technical measures processors and controllers can take to mitigate the resulting high data protection risks*[178]

The assessment must include:

- The relevant laws
- The purposes for which the data are processed
- The categories of data transferred and their sensitiveness
- Whether the data will be stored in the third country or whether there is remote access to data stored within the EU/EEA
- Role of the parties (public/private, processor/controller)
- All actors, including subprocessors
- The format of the data
- Possibility of onward transfers[179]

The relevant laws are outlined in Table 4 in this report. The purposes for which the data are processed, are limited to six technically necessary purposes to provide the requested communications, file sharing and storage functionality. Organisations may process all kinds of different categories of data via Zoom Meetings: ranging from public information to sensitive and special categories of data. The DTIA shows that the outcome of the risk assessment in this case is most dependent on the categories of data, and the format of the data (encrypted/anonymised/pseudonymised).

The risk assessment takes the differences into account between (i) laws governing US law enforcement access to remotely stored data, (ii) surveillance laws aimed at foreigners, such as FISA Section 702, and (iii) 'regular' FISA warrants for metadata, wiretaps, pen registers and business records.

While FISA Section 702 orders can theoretically be challenged by non-US persons through civil actions under the Administrative Procedure Act, it is very unlikely that such individuals are informed that their data have been accessed. Without such a notice, individuals don't know, and cannot seek redress.

Additionally, the protection of the Fourth Amendment of the US Constitution, which prohibits "unreasonable searches and seizures" and requires that a warrant must be based upon "probable cause" extends only to US nationals and citizens of any nation residing within the US. According to the

[178] EDPB, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, Version 2.0, Adopted on 18 June 2021, URL: https://edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf.

[179] Idem, p. 15.

US Supreme Court, foreigners who have not previously developed significant voluntary connections with the US cannot invoke the Fourth Amendment.[180]

The EU Court's assessment of the U.S. security agencies' bulk searches in the Schrems-II ruling implies that providers such as Zoom cannot guarantee an adequate level of protection because they cannot oppose FISA Section 702 orders or otherwise in all circumstances provide effective measures against the interference created by the law of the USA with the fundamental rights of persons whose data are transferred to the U.S.A.

EU individuals have more redress options against US law enforcement orders based on ECPA. ECPA protects 'persons', including foreign nationals, and recovering damages does not require proof of actual harm.

US CLOUD Act orders are somewhere in the middle. Different from national security orders and letters, providers are permitted to provide notice to their customers about CLOUD Act orders and 'regular' FISA warrants, unless the government has obtained a gagging order. CLOUD Act requests and gagging orders must be authorised by judges, but the redress possibilities for non-US persons are still wafer thin, as they will only be informed about orders for their data based on the US Cloud Act if the data are used in a criminal case.[181]

Absent a specific agreement with the EU or with individual EU countries, there is still a conflict of law absent an EU-US agreement on the access to personal data in criminal matters. Therefore, it is unlikely requests under the US CLOUD Act comply with the European essential data protection guarantees.

8.3.2. Mitigating measure: encryption

One of the most effective measures to mitigate the transfer risks is the application of end-to-end-encryption (See Section 9.1 of this report). This means the provider cannot decipher the data, not even under legal or illegal pressure. The DTIA assesses the risks of the application of bulk interception of the traffic in transit from the EU to the USA, based on E.O. 12333 as mitigated by PPD-28. The chance that surveillance authorities will obtain legible personal data from Meetings is calculated as zero when calculated over a two-year period. This is due to the E2EE of all Content Data in transit between the EU and the US. Therefore, the DTIA concludes that organisations can use Zoom to exchange highly sensitive and special categories of data through Meetings and encrypted chat when they apply E2EE.

Zoom encrypts all other personal data in transit with its own key. This also limits the risks for access by surveillance authorities in legible format.

The DTIA does include the small risk that US surveillance authorities are so interested in a particular individual, that there is a 5% chance that the personal data (including the E2EE Content Data) are the subject of intelligence searches. It is plausible that some Content Data exchanged via Zoom Meetings

[180] Quote from the Ad-Hoc-EU-US Working Group on Data Protection, quoted by Ian Brown and Douwe Korff in their study about transfers for the LIBE committee of the EP.

[181] See ECJ, Schrems-II, par. 181 and 182. U.S. surveillance programs conducted under Section 702 of the Foreign Intelligence Surveillance Act (FISA) and EO 12333 do not grant surveilled persons actionable rights before the courts against the US authorities / rights which are enforceable against the US authorities in the courts.

by an EU government or university organisation are considered interesting for intelligence searches, since data exchanged via the browser (instead of the Zoom client) cannot be e2e encrypted. The DTIA does not calculate the risk of decryption capacities in 10 or 20 years from now, or the likelihood of the assumption that the NSA is storing all intercepted metadata for future decryption purposes, as these assumptions are impossible to test or quantify.

8.3.3. Mitigating measure: transparency

Another important mitigating measure is if the transparency reports from the provider show that the practical chance of occurrence of this risk is almost zero, even though a low number of requests by itself cannot be used to assess the risk for data subjects as low.

The EDPB writes: "*you may decide to proceed with the transfer without being required to implement supplementary measures, if you consider that you have no reason to believe that relevant and problematic legislation will be applied, in practice, to your transferred data and/or importer. You will need to have demonstrated and documented through your assessment, where appropriate in collaboration with the importer, that the law is not interpreted and/or applied in practice so as to cover your transferred data and importer, also taking into account the experience of other actors operating within the same sector and/or related to similar transferred personal data and the additional sources of information described further below that relevant and problematic legislation will be applied, in practice, to your transferred data and/or importer.*"[182]

As explained in Section 6.3.1 Zoom twice per year publishes a detailed transparency report about the amount of law enforcement requests and surveillance orders it has received. While taking into account that Zoom is not allowed to disclose the precise numbers of national security orders it has received, Zoom does not mention any US Cloud Act, FISA 702 or National Security Letters at all. Zoom estimates the number of requests in the DTIA to be 0.5 per year based on historical experience. Therefore, the number of requests for personal data based on these powers is assumed to be zero.

With the examples of the meetings organised by a US University, and a US cryptocurrency company, Zoom has explained why it cannot distinguish between the EU or US American origin of its customers. Zoom therefore cannot disclose how many of the 'regular' US law enforcement orders may incidentally include personal data from participants with an EU Education or Enterprise account. Zoom has disclosed to SURF that it never yet has received a specific order, warrant or subpoena for personal data of an EU Education or Enterprise customer. Therefore, the risk is assessed as 0.5 case per year, for all the different categories of personal data, assessed in the different tabs in the Excel sheet with the DTIAs.

When the Dutch universities and government organisations rely on the assessment that the transfer of some pseudonymous personal data can be allowed without E2EE, the EDPB warns they are not allowed to only rely on information about documented practical experience of Zoom with relevant prior instances of requests for access received from public authorities in the third country. They must also do a comparative analysis with other available types of "*relevant, objective, reliable, verifiable and publicly available or otherwise accessible information on the practical application of the relevant law (e.g. the existence or absence of requests for access received by other actors operating within the*

[182] EDPB Recommendations on supplementary measures, par 43, p. 18.

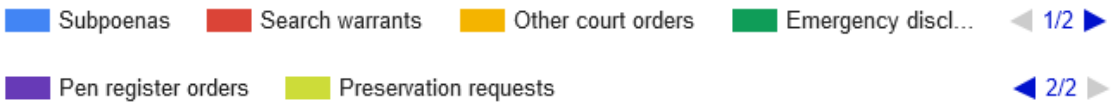
same sector and/or related to similar transferred personal data and/or the application of the law in practice, such as case law and reports by independent oversight bodies." Zoom's competitors for communication and business-to-business storage services such as Microsoft, Google, AWS, and Cisco have also published information about the number of US government requests they have received.

Microsoft publishes extensive transparency reports, distinguishing between law enforcement and security requests, and between consumers and Enterprise/Education customers. The number of requests for data from Enterprise customers is very low to the requests for consumer data. Microsoft writes: "*the overwhelming majority of requests seek information related to our free consumer services. By comparison, we have received very few requests for data associated with use of our commercial services used by enterprise customers.*"[183]

With regard to disclosures under the US Cloud Act, Microsoft writes it only complied once with such a request in the second half of 2020 relating to a non-US Enterprise customer, and with two such requests in the first half of 2021. These disclosed data do not necessarily have to be from a European customer: "*In the same time frame, Microsoft received 120 legal demands from law enforcement in the United States for commercial enterprise customers who purchased more than 50 seats. Of those demands, 2 warrants resulted in disclosure of Content Data related to a non-US enterprise customer whose data was stored outside of the United States.*"[184] These two cases do not necessarily involve EU Customers, but may very well involve customers in Asia, South America or Africa, as Microsoft also ensures it has never disclosed personal data from any EU public sector customer to any government.

Google, like Microsoft, also distinguishes between consumer and Enterprise accounts.[185] Though Google has received 185 requests in total in the second half of 2020, this does not mean Google has provided data in all of these cases. More importantly, Google does not explain where these Enterprise customers are located.

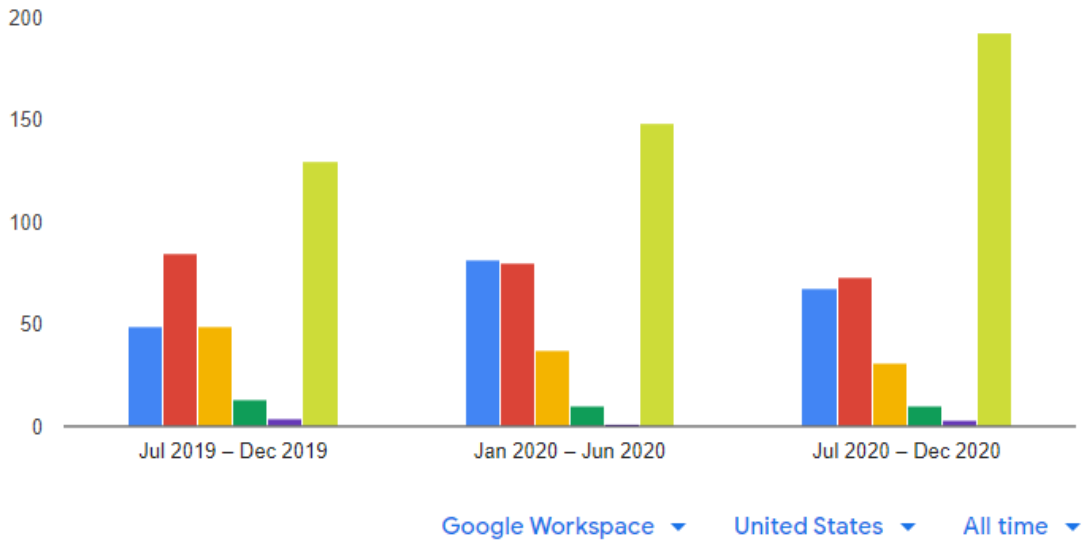
Figure 23: Google statistics US law enforcement requests for global Enterprise customers



[183] Microsoft blog, Q: What services are subject to law enforcement requests?, undated, https://blogs.microsoft.com/datalaw/our-practices/#does-microsoft-reject-us-subpoenas-from-government-seeking-content-data.

[184] Idem, answer to the question: "Does Microsoft disclose additional data as a result of the CLOUD Act?"

[185] Google Transparency Report, Enterprise cloud requests for customer information, URL: https://transparencyreport.google.com/user-data/enterprise?hl=en_GB.



Competitor Cisco also publishes bi-annual transparency reports.[186] Similar to Microsoft's and Google's reporting, Cisco also provides many different services, not limited to online communication and cloud recording services. In the first half of 2021, Cisco disclosed non-Content Data in 7 cases on demands from US law enforcement. For US national security demands. Cisco only reports in ranges, like Microsoft and Google, between 0 and 249 cases.

[186] Cisco Transparency Report Jan-June 2021, URL: https://trustportal.cisco.com/c/r/ctp/trust-portal.html?search_keyword=transparency#/1640125994492149.

Figure 24: Cisco statistics US law enforcement requests for global Enterprise customers

Reporting Period: January 1st -June 30st, 2021

Government Data Demands – United States (exclusive of National Security Demands, which are reported below)

Data Type Demanded	Total Demands	No Data Found	Total Rejected	Total Disclosed
Content Data	5	4	1	0
Non-Content Data	25	13	5	7
Emergencies	0	0	0	0

United States National Security Demands

Cisco may receive demands for data from U.S. national security organizations. These include Foreign Intelligence Surveillance Act (FISA) warrants, orders, directives, or National Security Letters (NSLs). The table below lists the number of U.S. National Security demands Cisco has received during the applicable period, subject to the limitations prescribed by the USA Freedom Act of 2015.

January 1st -June 30st, 2021	Totals
National security orders, directives, or national security letters received	0-249
Number of accounts affected under all national security orders, directives, or national security letters	0-249

In response to the decision from the Austrian DPA that a website could no longer use Google Analytics, because of the transfer of (pseudonymised) data to Google's servers in the USA, Google wrote: "*But Google has offered Analytics-related services to global businesses for more than 15 years and in all that time has never once received the type of demand the DPA speculated about. And we don't expect to receive one because such a demand would be unlikely to fall within the narrow scope of the relevant law*."[187]

Another US business to business company, IBM, has for example explained that it has only received 1 CLOUD Act request, and refused to comply. The company explains it has never provided client data stored outside of the US to the US government under any national security order, including FISA warrants.[188]

AWS provides the clearest assurance about the disclosure of Enterprise Content Data located outside the United States, namely: zero, both in the first and second half of 2021.[189] However, AWS did receive

[187] Google in Europe, It's time for a new EU-US data transfer framework, 19 January 2022, URL: https://blog.google/around-the-globe/google-europe/its-time-for-a-new-eu-us-data-transfer-framework/.

[188] Computer Weekly, IBM pushes back against US government data requests, 7 June 2021, URL: https://www.computerweekly.com/news/252501996/IBM-pushes-back-against-US-government-data-requests.

[189] AWS Information Requests Report June-December 2021, published 31 January 2022, URL: https://d1.awsstatic.com/Information_Request_Report_December_2021_bia.pdf.

a total of 393 requests from US law enforcement in the second half year of 2021, and 390 such requests in the first half of 2021. AWS does not explain how many of these requests related to Non-Content data from customers in the EU. AWS also reports a range of 0-249 national security requests.

Figure 25:AWS answer to question about access to Content Data outside the US[190]

How many requests resulted in the disclosure to the U.S. government of enterprise content data located outside the United States?
None.

Published January 31, 2022

In sum, based on Zoom's transparency reporting, and compared to larger US companies in the same sector that process similar transferred personal data, the estimated number of 0.5% US law enforcement and security orders combined per year for personal data from Zoom's EU Education and Enterprise customers seems plausible.

8.3.4. Mitigating measure: pseudonymisation and aggregation

Even if the Content Data are encrypted with keys controlled exclusively by the customer, the Diagnostic, Account and Support Data contain all kinds of identifiable data and contents such as meeting names and participant names. Though Zoom applies encryption, both in transit and at rest, Zoom needs to process most of these data in the clear to provide the requested services.

The subset of Telemetry Data is collected in a pseudonymised format. As described in Section 3.2 Zoom only collects 49 different Telemetry Events with very limited information. The events do not contain Content Data, or information about other users, meeting names or other user-supplied values such as profile names.

Once Zoom has completed its EU Cloud, by the end of 2022, Zoom may continue to transfer some Diagnostic Data to its USA Trust & Safety Team. However, Zoom will only transfer a pseudonymised identifier, which can be combined with other data about the usage. Zoom will minimise access authorisations and limit the storage of these events to max. 180 days. In reply to this Update DPIA Zoom has further committed to consider a solution not involving physical transfer, by either devoting EU staff to this task, or developing a secure terminal option that does not allow for exports of the personal data.

8.3.5. Other mitigating measures: EU Support and EU Cloud

Zoom has committed to develop EU data localisation for its EU Education and Enterprise customers, by the end of 2022, and offer an EU-only choice for Support Data by mid-2022.

When Zoom indeed exclusively processes all personal data (except pseudonymised Diagnostic Data for its Trust & Safety Team) within the territorial boundaries of the EU, while it continues to offer E2EE and apply effective transit encryption, the risks of mass surveillance by the US security services are negligible. Of course, US authorities could still order access to personal data from individuals hosted in the EU, but the chance that Zoom will disclose such data can be assessed as unlikely, also in view of Zoom's obligation in the SCC to inform the controller of its inability to comply with the standard data

[190] Similarly, AWS writes 'None' in the information request report about January to June 2021, URL: https://d1.awsstatic.com/Information_Request_Report_June_2021_x.pdf.

protection clauses, even when it is prohibited from informing its customer in the EU that it has received a legally binding request for disclosure of personal data.[191]

As quoted in Section 6.3.1, Zoom commits in the DPA to judicially object to requests or orders or the prohibition to inform the Controller about this or to follow the instructions of the Controller.

8.3.6. Future developments: EDPS investigation and coordinated EDPB cloud investigation

On 27 May 2021 the EDPS announced it would start an investigation to verify compliance with its Recommendations[192] on the use of Microsoft Office 365 as contracted by the European Commission, and into the legitimacy of data transfers by public cloud infrastructure services offered by Microsoft (Azure) and Amazon (Amazon Web Services).[193]

The EDPS explains: "*These investigations are part of the EDPS' strategy for EU institutions to comply with the "Schrems II" Judgement so that ongoing and future international transfers are carried out according to EU data protection law.*"[194] The outcomes of these investigations are relevant to understand how the EDPD will assess the risks of the transfer of pseudonymous personal data to Zoom that are not E2EE, and the commitment to develop an EU cloud. No results have yet been published.

On 18 October 2021 the EDPB announced its first coordination on the use of cloud based services by the public sector. The EDPB explains: "*In a coordinated action, the EDPB prioritizes a certain topic for supervisory authorities to work on at the national level. The results of these national actions are then bundled and analysed, generating deeper insight into the topic and allowing for targeted follow-up on both the national and the EU level the joint task force.*"[195] The head of this taskforce, Gwendal le Grand, wrote: "*In the first quarter of 2022, we will announce further details on the first topic that was chosen for coordinated action within the CEF, namely the use of cloud services by the public sector. The EDPB prioritized this topic because the increasing deployment of cloud services in the public sector triggers a number of data protection risks which require careful assessment.*"[196]

---

[191] EDPB, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, footnote 98, p. 39.

[192] EDPS, Outcome of own-initiative investigation into EU institutions' use of Microsoft products and services, 2 July 2020, URL: https://edps.europa.eu/data-protection/our-work/publications/investigations/outcome-own-initiative-investigation-eu_en.

[193] EDPS press release, The EDPS opens two investigations following the "Schrems II" Judgement, 27 May 2021, URL: https://edps.europa.eu/press-publications/press-news/press-releases/2021/edps-opens-two-investigations-following-schrems_en.

[194] Idem.

[195] EDPB, EDPB launches first coordinated action, 18 October 2021, URL: https://edpb.europa.eu/news/news/2021/edpb-launches-first-coordinated-action_en.

[196] EDPB, EDPB Support Pool of Experts: enhancing cooperation by complementing the strengths of SAs, 11 January 2022, URL: https://www.linkedin.com/pulse/edpb-support-pool-experts-enhancing-cooperation-complementing-/?trackingId=I0uTg7jPQHW6c1qQ%2FGJSzA%3D%3D.

On 15 February 2022 the Dutch Data Protection Authority published a press release about its participation in the joint task force[197] It announces an EU-wide questionnaire, and explains that the EDPB will issue a joint report about the outcomes by the end of 2022.

It is uncertain how the transfer risks will be assessed by the national data protection authorities in this joint investigation. For this DPIA the transfer risks have been rigorously assessed, including a separate DTIA. Zoom has committed to follow recommendations from the EDPB, and to loyally collaborate with SURF and the Dutch government to update the DTIA when necessary.

The outcomes of this DPIA must be reassessed if the EDPS and/or the EDPB taskforce come to a different conclusion with regard to the high and low risks, especially regarding the ongoing (limited) data transfer to the USA and the mitigating measures described above.

9. Techniques and methods of the data processing

As explained in Section 1 of this report, Zoom collects and generates personal data in multiple ways. Zoom collects Content Data, Account Data, Support Data and Feedback Data when they are submitted or sent by or on behalf of customers. In addition, Zoom collects and generates Diagnostic Data, (including Telemetry Data and metadata about filed support requests) and Website Data (including cookies) about the use of its services and software.

9.1. Types of encryption

By default, Zoom applies industry standard encryption to the connection between end-user devices and Zoom, "*using a mixture of TLS (Transport Layer Security), Advanced Encryption Standard (AES) 256-bit encryption, and SRTP (Secure Real-time Transport Protocol). The precise methods used will depend on whether you are using the Zoom client, a web browser, a third-party device or service, or the Zoom phone product.*"[198] In its FAQs about transfers of personal data to the USA after the Schrems II ruling, Zoom explains it also encrypts all cloud recordings with its own keys. "*Encryption of recordings: All cloud recordings are encrypted using AES 256-bit encryption with complex passwords on by default.*"[199]

In November 2020 Zoom launched end-to-end encryption (E2EE) of the streaming audio and video in Zoom Meetings. Though Zoom meetings are encrypted by default with Zoom-controlled keys, enabling the E2EE offers important extra assurances for the processing of personal data, as only the end user

[197] Dutch DPA (in Dutch only), Privacytoezichthouders onderzoeken gebruik clouddiensten door overheidsinstellingen, URL: https://www.autoriteitpersoonsgegevens.nl/nl/nieuws/privacytoezichthouders-onderzoeken-gebruik-clouddiensten-door-overheidsinstellingen.

[198] Idem.

[199] Zoom, FAQS: Transferring EEA & UK Residents' Data to the US.

controls the key for the decryption. The use of E2EE has some usage disadvantages as well, as noted in Section 4.2.1.

Admins can also enable Advanced chat encryption. Zoom explains: "*When advanced chat encryption is enabled, Content Data at rest is encrypted by keys generated & operated on chat participants' devices.*"[200]

Zoom explains the difference between Zoom's regular encryption and E2EE:[201]

"*How is this different from Zoom's enhanced GCM encryption?*

Zoom meetings and webinars by default use AES 256-bit GCM encryption for audio, video, and application sharing (i.e., screen sharing, whiteboarding) in transit between Zoom applications, clients, and connectors. In a meeting without E2EE enabled, audio and video content flowing between users' Zoom apps is not decrypted until it reaches the recipients' devices. However, the encryption keys for each meeting are generated and managed by Zoom's servers. In a meeting with E2EE enabled, nobody except each participant – not even Zoom's servers – has access to the encryption keys being used to encrypt the meeting."

As a general caveat, E2EE is an important measure against interception by third parties and the consequences of a security incident. However, the customer needs to be able to trust Zoom. It is possible for Zoom or coders that work for Zoom, by way of example, not as an allegation, to insert backdoors in its software and retrieve the encryption keys. This caveat applies to all cloud providers. In its reply to this DPIA, Zoom contests the importance of this risk. "*The main threat model E2EE guards against is someone siphoning data at the server. For those with concerns about backdoors, Zoom makes its client-side code available to third-party auditors, commissioned both by customers and by ourselves.*"[202] However, to alleviate any concerns from its customers, Zoom has added the following guarantees to its DPA:

"Zoom may not update the Services in a way that would remove Customer's choice to apply end to end encryption to Meetings, introduce any functionality that would purposefully allow anyone not authorized by the Customer to gain access to Customer encryption keys or customer content, or remove the ability to store recordings locally.

To the best of its knowledge, Zoom certifies that it has not purposefully created any "back doors" or similar programming in the Services that could be used by third parties to access the system and/or personal data. Zoom has not purposefully created or changed its business processes in a manner that facilitates such third-party access to personal data or systems. Zoom certifies there is no applicable law or government policy that requires Zoom as importer to create or maintain back doors or to

[200] Zoom, Advanced chat encryption, 1 February 2022, URL: https://support.zoom.us/hc/en-us/articles/207599823.

[201] Zoom End-to-end (E2EE) encryption for meetings, last updated 14 January 2022, URL: https://support.zoom.us/hc/en-us/articles/360048660871-End-to-end-E2EE-encryption-for-meetings.

[202] Zoom reply to part A of the DPIA, 19 March 2021, p. 84.

facilitate access to personal data or systems or for the importer to be in possession of or to hand over the encryption key." [203]

The E2EE protection is available for streaming Content Data, but not for cloud recordings and cloud transcriptions. As quoted above, Zoom encrypts such files by default with AES 256-bit encryption, but different from E2EE, Zoom has access to the keys. Customers can choose to store cloud recordings locally, on their own devices/in their local data centre, and apply their own encryption tools.[204]

E2EE is not possible for the processing of metadata. As evidenced in Section 3.1, Diagnostic Data may reveal sensitive or confidential information about meetings or qualifications about participants.

In sum, the application of E2EE and Advanced Chat encryption is a necessary functionality, but not the answer to all problems with the transfer of personal data to a country without an adequate data protection regime.

9.2. Anonymisation

According to the guidance from the Data Protection Authorities in the EU, anonymisation is a complex and dynamic form of data processing. [205] Often, organisations still possess original data, or continue to collect pseudonymised data.

As long as there is a realistic possibility to re-identify individuals based on data that are masked, scrubbed from obvious identifiers or otherwise de-identified, such data cannot be considered anonymous and the organisation must still comply with all GDPR requirements with regard to the processing of personal data. Furthermore, the process of anonymization constitutes processing of personal data and is therefore subject to the GDPR.

The removal (erasure or deletion) of personal data after its collection also constitutes processing of personal data subject to the GDPR. The fact that Zoom may delete certain personal data from the Diagnostic Data, may apply aggregation techniques, makes no difference to the assessment that Zoom processes personal data via these log files.

In reply to the first DPIA, Zoom has added a definition of 'anonymisation' to its DPA, stopped using the confusing term 'de-identify', and has agreed to precisely define in the DPA when it may process directly identifiable data, and when only aggregated data. The term 'aggregated' is further specified, that it may never reference to an individual customer.

9.3. Privacy by design and privacy by default

The first DPIA concluded that Zoom already processed personal data with many privacy friendly default settings for admins and for end users, as shown in Sections 4.1 and 4.2.

---

[203] Zoom new DPA, Clauses 6.1 and 6.2.

[204] Zoom, Protection your data, URL: https://zoom.us/trust/security.

[205] Anonymisation Guidelines from the Article 29 Working Party, WP216, Opinion 05-2014 on Anonymisation Techniques, URL: http://ec.europa.eu/justice/Article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf.

In dialogue with SURF after the first DPIA Zoom has taken or committed to take additional measures to comply with the principles of privacy by design and privacy by default (Art. 25 GDPR).

In the DPA, Zoom commits to maintain the following measures and principles:

- Zoom agrees to minimise the data processing to the extent strictly necessary to provide the contracted services. This includes minimisation of information collected via Telemetry Data, Support requests and Feedback functionality, minimisation of data retention periods, collection of pseudonymised identifiers, when necessary, but immediate effective (irreversible) anonymisation when the service can be performed without personal data, offer end-to-end-encryption when technically feasible, and the implementation and control of strict access controls to the Customer Data.[206]
- Zoom shall implement policies whereby when Zoom collects new types of Diagnostic Data, such new collection shall be supervised by a Privacy Officer. Zoom will perform regular checks on the contents of collected Telemetry Data to verify that no directly identifying data are collected nor Content Data.[207]
- With regard to Zoom's use of cookies or similar tracking technology, Zoom shall ensure that only those cookies which are strictly necessary shall be set by default for European Enterprise and Education Customers on zoom.us, support.zoom.us and explore.zoom.us, including visits to these pages when the End User or system administrator has signed-in to the Zoom account.[208]
- When Zoom plans to introduce new features, or related software and services ("New Service") that will be offered within the scope of the contracted Enterprise or Education license and will result in new types of data processing (i.e., new personal data and/or new purposes), Zoom will:
    - Perform a Data Protection Impact assessment.
    - Determine if the new types of data processing following a New Service are allowed within the scope of this Addendum.
    - Ensure that the new data processing will only start after an opt-in given by the Customer (the admin, never the end user).
    - Zoom agrees to only transfer pseudonymised Diagnostic Data to the USA, and scrub any Content Data from Diagnostic Data if accidentally included in logs such as SIEM logs.[209]

[206] Zoom new DPA, Clause 3.2.

[207] Zoom new DPA, Clause 3.3.

[208] Zoom new DPA, Clause 3.4.

[209] Zoom new DPA, Clause 3.5.

10. Additional legal obligations: e-Privacy Directive

This section only describes the additional obligations arising from the current ePrivacy Directive and (possible) future e-Privacy Regulation. In view of the limited scope of this DPIA, other legal obligations or frameworks (for example in the area of information security, such as BIO) are not included in this report.

Certain rules from the current ePrivacy Directive apply to the storage of information on, and retrieval of that stored information from, browsers with pixels and cookies and similar technologies such as tracking pixels and unique identifiers sent through URL parameters. These rules also apply to software installed on devices that sends information via the Internet through an inbuilt telemetry client. Article 5(3) of the ePrivacy Directive was transposed in Article 11.7a of the Dutch Telecommunications Act. Consent is required prior to the retrieval or storage of information on the devices or browsers of end users, unless one of the exceptions applies, such as the necessity to deliver a requested service, or necessity for the technical transmission of information.

The consequences of this provision are far-reaching, as it requires clear and complete information to be provided to the end user prior to data processing, as well as consent, unless one of the legal exceptions applies.

This consent requirement applies to all tracking cookies on the Zoom website. The Dutch implementation of the ePrivacy cookie rules has a specific legal assumption that tracking cookies involve the processing of personal data. Hence, the GDPR automatically also applies. As analysed in Section 3.4 of this report, both the publicly accessible parts, and the restricted access parts of the Zoom website currently place and read information from end-user devices (cookies and other trackers).

In reply to the initial DPIA, Zoom has applied a new cookie consent banner, and has gradually removed a few remaining cookies or traffic to third parties from the strictly necessary level. Zoom does not use the IAB consent framework that has very recently been declared unlawful by the Belgian DPA.[210] Zoom has drafted a new Cookie Statement, and has added a warning to its EU website visitors that they consent to the transfer of data to the USA when they consent to cookies different from the default strictly necessary cookies.

As last checked by Privacy Company at the end of January 2022, Zoom's cookie practice seems compliant with Article 11.7a of the Dutch Telecommunications Act and with the GDPR requirements

[210] Belgian DPA, The BE DPA to restore order to the online advertising industry: IAB Europe held responsible for a mechanism that infringes the GDPR, 2 February 2022, URL: https://www.dataprotectionauthority.be/citizen/iab-europe-held-responsible-for-a-mechanism-that-infringes-the-gdpr and IAPP, Belgian DPA fines IAB Europe 250K euros over consent framework GDPR violations, 2 February 2022, URL: https://iapp.org/news/a/belgian-dpa-fines-iab-europe-250k-euros-over-consent-framework-gdpr-violations/.

for this type of personal data processing. This includes transparency about the strictly necessary cookies. Zoom's cookie consent banner provides a full overview of the identity, name, purpose and retention period of each category of cookies.

The legal consent requirement is not limited to the tracking cookies. Zoom must also ask for consent for the collection of Telemetry Data from the Zoom apps. As described in Section 3.2, even though Zoom collects minimal information through the current telemetry, the processing does include usage data, unique identifiers and timestamps. In reply to the finding of a lack of transparency in the initial DPIA, Zoom has published a Privacy Data Sheet with detailed event level information about the telemetry events it collects.

Figure 26: Timeline new ePrivacy Regulation

The current ePrivacy Directive also includes rules on the confidentiality of data from the content and on communication behaviour. Article 5(1) obliges Member States to guarantee the confidentiality of communications and related traffic data via public communications networks and publicly available electronic communications services. Article 6(1) obliges providers of publicly available telecommunications services to erase or make the traffic data anonymous as soon as they are no longer needed for the purpose of the transmission of the communication.

Although the confidentiality rules in the ePrivacy Directive originally only covered classic telephony and internet providers, the scope was expanded significantly last year. Since the European Electronic Communications Code (EECC) became applicable law (21 December 2020) , the confidentiality rules apply to all over-the top communications services, such as Zoom and other providers of internet-based videoconferencing and chat services.

The consent requirement for tracking cookies will likely continue to exist in the future ePrivacy Regulation.

On 10 January 2017, the European Commission published a proposal for a new ePrivacy Regulation. This was followed by an intense political debate the last four years. The European Parliament responded quickly and positively, but it has taken the representatives of the EU Member States three years to draft a compromise about the proposed ePrivacy Regulation.

The Council sent its agreed position to COREPER to start the trialogue on 10 February 2021.[211] The most recent update from the Council dates from 12 November 2021.[212] In the first half of 2022, France has announced ePrivacy will be a priority during its Presidency of the Council.[213] The points of view of the European Parliament and the European Council are widely diverging. Therefore, it is not likely that the ePrivacy Regulation will enter into force anytime soon, and Zoom will have to comply with the current ePrivacy and EECC rules in the next few years.

11. Retention periods

In response to the findings in the initial DPIA, Zoom has committed to an overhaul of its data retention policy, and to shorten retention periods. Zoom commits to retain new data from Dutch university and government customers no longer than 12 months after they sign up for the new DPA, unless otherwise mentioned in the table below.

Zoom will gradually work backward to remove all existing older data from all its systems, and work on a generalized retention scheme for all its EU Enterprise and Education customers.

Zoom has provided detailed information about its own retention periods for the different kinds of personal data it collects and stores, as shown in Table 5 below.[214] Customers can apply their own retention periods to personal data under their control, such as cloud recordings.

Table 5: Zoom data retention periods

Meeting and Webinar Content Data	
Data Type	Timeline for Deletion
User or Account Profile Information (first and last name, login and password (if SSO is not used), display name, phone (optional), social media login (optional), profile picture (if provided), department (if provided), + the Zoom attributed unique User ID	Account profile information (such as social media login, profile picture, password) is deleted when the user account is deleted. *Some information (such as username and display name) may be retained for up to 12 months if associated with a meeting of an active user account.
Cloud Recordings (includes closed captioning, live transcripts, recording highlights and chat transcripts)	Information is retained as long as the user has an active account *Retention for cloud recordings can be set at the user's group or at the account level by an administrator's discretion.

[211] Council of the European Union, Interinstitutional File 2017/0003(COD), Brussels, 10 February 2021 (OR. en) 6087/21, URL: https://data.consilium.europa.eu/doc/document/ST-6087-2021-INIT/en/pdf.

[212] Council of the European Union, Interinstitutional File 2017/0003(COD), Brussels, 12 November 2021, request for an amended mandate, largely blacked out, URL: https://data.consilium.europa.eu/doc/document/ST-13558-2021-INIT/en/pdf.

[213] French Presidency of the Council of the European Union, Programme of the Presidency, URL: https://presidence-francaise.consilium.europa.eu/en/programme/programme-of-the-presidency/.

[214] Zoom Data Retention and Deletion Standards for Zoom Accounts purchased by SURF/HEAnet and the Dutch government, Version 1.0, 24 January 2022.

Cloud recording raw files [215]	15 days after the date of collection
Polling questions and responses (optional)	12 months from the date of collection
Webinar questions and answers (optional)	12 months from the date of collection
Persistent Chat Messages	12 months from the date of collection
In-Meeting Chat Messages (in-meeting group chat messages that are not transferred to a permanent chat channel and in-meeting 1:1 chats)	Immediately after the meeting ends *If cloud recording is enabled, a transcript of public chat messages can be saved on the cloud and retention will follow 'Cloud Recordings'. Private messages between participants are not saved.
Meeting & Webinar registration data	12 months from the date of collection
Files & Images (exchanged in meeting)	Within 24 hours after the meeting
Calendar Information (includes contact information made available through Customer controlled integrations e.g., Outlook, Google Calendar)	12 months from the date of collection
Trust & Safety Data	180 days from the date of collection
PhotoDNA matches (on files uploaded to persistent Chat, Zoom Room backgrounds, and profile pictures)	180 days from the date of collection
SPAM identification	180 days from the date of collection
Meeting and Webinar Support Data	
Data Type	Timeline for Deletion
Support Data (includes contact name, time, subject, problem description)	180 days after ticket is closed
Support Data Attachments	Within 24 hours after ticket is closed
Meeting and Webinar Diagnostic Data	
Data Type	Timeline for Deletion
Meeting or Webinar Metadata[216]	12 months from the date of collection.
Telemetry Data	12 months from the date of collection
Other Service Generated Data	12 months from the date of collection
IP addresses (US fiscal law[217])	6 years, but Zoom plans immediate anonymisation, with extraction of country, pending legal authorisation
Website Data	
Data Type	Timeline for Deletion
Zoom web server access log for both public and restricted access website (after log-in)	18 months
Strictly necessary cookies on Zoom website	From a few seconds to 2 years: see Zoom List of Strictly Necessary Cookies in the Cookie Preference Center and the Zoom Cookie Policy at https://explore.zoom.us/en/cookie-policy/

[215] Defined by Zoom as "raw files (without being compressed or edited to fit into other file formats) generated when a customer initiates a cloud recording. These files are processed to .mp4, .m4a, .vtt, .cc.vtt, or .txt for customer use.

[216] Defined by Zoom as: "*information about the deployment of Zoom Services and related systems environment / technical information). This will include IP addresses, Data center, PC name, Microphone, Speaker, Camera, Domain, Hard disc ID, Network type, Operating System Type and Version, Client Version, Service Version, Geographic Region.*".

[217] Based on US Treasury Regulation 1.250(b)-5(e) for services provided to businesses.

Zoom EU customer Vanity URL access logs	3 months
	Backups
Data Type	Timeline for Deletion
Zoom meeting & webinar database backup	Within 35 days

11.1. Content Data

If a customer actively deletes Content Data (including terminating an account) the data will be deleted within 31 days from Zoom's servers.

Files and images exchanged in both recorded and unrecorded meetings are deleted within 24 hours after the meeting. In reply to the initial DPIA, Zoom wrote it had considerably shortened the retention period from 31 days to max. 24 hours: "*Zoom retains Files and Images that are exchanged via in-meeting chat so other participants can download it from our servers. I understand that we now delete this data within 24 hours.*"[218]

Zoom stores the cloud recordings as long as the university or government organisation remains a customer of Zoom Meetings Enterprise. With Cloud Recordings, Zoom means Mp4 of all video, audio and presentations, M4A of all audio, the text file of all in meeting chats, and audio transcript files. Customers can determine their own retention periods for cloud recordings.

Zoom will remove deleted Content Data from its backups after 35 days.

11.2. Diagnostic Data

In its data retention table, Zoom describes three categories of diagnostic data, namely:

1. Meeting or Webinar Metadata
2. Telemetry Data
3. Other Service Generated Data

All three categories are retained for 12 months after collection. Additionally, Zoom collects Structured data that is generated by the user when using the service. Zoom describes these user activity logs as 'Other Service Generated Data' in its retention table and will retain the data for 12 months after creation/collection.

Administrators may have access to the following user activity logs in the web portal.

- Operation Logs,
- Sign-in/Sign-out Logs and
- User Disclaimer Logs.

Zoom explained that system logs can be both unstructured and structured. System logs are generally created in an unstructured format, but could be proliferated into structured data for troubleshooting. Unstructured Data is "*Data that cannot be viewed by Subscriber in the Service and*

[218] Zoom reply to part A of the DPIA, 19 March 2021, p. 88.

includes data that, for example, is maintained in infrastructure logs." Zoom will retain all logs (whether structured or unstructured) for 12 months after creation/collection.

11.3. Account Data

Zoom distinguishes between the paid account holder data (i.e., such as a software procurement officer at a university), and Account Data of end-users and admins that are not also owners of the contract with Zoom.

1. Account Holder Data: Zoom (as an independent data controller) retains the sales and billing contact data for a period of 10 years.

2. Account Data end users: Zoom retains the end-user Account Data as long as the employee works for the same organisation, plus 31 days. Admins can remove the Account Data of a (group of) end users, but Zoom does not yet offer a tool to delete all related personal data to an account, such as Diagnostic Data. As a result of the discussions with SURF, Zoom has committed to provide a tool for admins to individually delete end user Diagnostic Data by the end of 2022.

Some information (such as username and display name) may still be retained in other Diagnostic Data for up to 12 months if associated with a meeting of another active user's account.

11.4. Website Data

Zoom defines *Website Data* as information collected when a user interacts with Zoom's websites through strictly necessary cookies (or optional cookies when a user provides consent). This information allows Zoom to measure and improve performance of the website and, if consent is provided, to personalise and enhance the user's experience. These data may include device information such as client IP address, request date/time, page requested, browser type, cookie values, navigator objects (i.e. screen resolution size) and hosts list. Additional user activity collected may include browsing history and search history on Zoom's website. Zoom is contractually authorised to aggregate the website data and store these aggregated data to conduct analytics and measure performance for longer than 18 months.

Part B. Lawfulness of the data processing

The second part of this DPIA assesses the lawfulness of the data processing. This Part B contains an assessment of the legal grounds for processing (Section 12), the processing of special categories of personal data (Section 13), the principle of purpose limitation (Section 14), an assessment of the necessity and proportionality of the processing (Section 15), and data subject rights (Section 16).

12. Legal Grounds

To be permissible under the GDPR, processing of personal data must be based on one of the grounds mentioned in Article 6 (1) GDPR. Essentially, for processing to be lawful, this article demands that the data controller bases the processing on the consent of the user, or on a legally defined necessity to process the personal data.

The assessment of available legal grounds (sometimes called 'lawful bases') is tied closely to the principle of purpose limitation. The EDPB notes that "*The identification of the appropriate lawful basis is tied to principles of fairness and purpose limitation. [.] When controllers set out to identify the appropriate legal basis in line with the fairness principle, this will be difficult to achieve if they have not first clearly identified the purposes of processing, or if processing personal data goes beyond what is necessary for the specified purposes.*"[219]

Thus, in order to determine whether a legal ground is available for a specific processing operation, it is necessary to determine for what purpose, or what purposes, the data was or is collected and will be (further) processed. There must be a legal ground for each of these purposes.

In the first DPIA on Zoom, Zoom was factually qualified as a joint controller with the universities and government organisations. Thanks to Zoom's improvement commitments, and the limitative list of purposes in the new DPA, Zoom's role is now clarified for the different purposes of the processing as either a processor, or a controller.

Section 12.1 discusses the legal grounds for the universities and government organisations as controllers, when Zoom is a processor. Additionally, through the DPA, EU Education and Enterprise customers authorise Zoom to 'further' process some personal data for six specific legitimate business purposes. Section 12.2 discusses Zoom's own legal grounds as an independent data controller for these six purposes.

The legal ground of vital interest is not discussed, since nor Zoom nor universities or Dutch government organisations have a vital (lifesaving) interest in processing personal data via Zoom

[219] EDPB, Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects - version adopted after public consultation, 16 October 2019, URL: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22019-processing-personal-data-under-article-61b_en.

Meetings.[220] Additionally, though organisations may efficiently work from home by organising video conference calls, there is no legal obligation to use Zoom Meetings (or other videoconferencing software).

12.1. Zoom as processor

Thanks to the improved DPA and Zoom's improvement measures, Zoom will only process the personal data it obtains from, through or about the use of its contracted services (the various video conferencing, web conferencing, webinar, meeting room, screensharing, chat, connectors, audio plans, cloud storage, and other collaborative services accessible through a web browser or a software application and related customer support that Customer may order) for five authorised purposes, when necessary. These five purposes are:

- Providing and updating the Services as licensed, configured, and used by Customer and its users,
- Securing and real-time monitoring the Services,
- Resolving issues, bugs, and errors,
- Providing customer requested support,
- Processing as set out in the Agreement and Annex I to the SCCs and other documented instruction provided by Customer and acknowledged by Zoom as constituting instructions for purposes of this Data Processing Agreement.[221]

The limitation in the DPA to these five purposes, together with the right to audit Zoom's compliance, ensures that Zoom behaves as a data processor for the **Content Data, Account Data, Diagnostic Data, Support Data, Feedback Data and (restricted access) Website Data**. As a processor, Zoom relies on the legal grounds the controllers have for the authorised purposes.

As data controllers for the processing of these personal data via Meeting, universities and government organisations can successfully appeal to four of the six possible legal grounds. These are discussed below.

12.1.1. Consent

Article 6 (1) a GDPR reads: "*the data subject has given consent to the processing of his or her personal data for one or more specific purposes." Based on Art. 4 (11) GDPR, consent means "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.*"

Employers should refrain from asking for consent from employees for the processing of their personal data. In view of the imbalance of power between employees and employers, between educational

[220] Of course, a university or government organisations can obtain information about a life-threatening situation during a Zoom Meeting, and feel compelled to share such information with a third party. In that case, the organisation needs to assess whether it can legitimately appeal to this legal ground for the specific disclosure. But such an assessment is separate from the legal ground to use Zoom Meetings in general.

[221] Zoom new DPA, Clause 2.2.

institutions and students, consent can seldom be given freely.[222] Employees and students may not be free to refuse or withdraw consent for the processing of their personal data without facing adverse consequences.

The fact that government organisations and most universities are public sector organisations also makes it difficult to rely on consent for processing. In the context of Recital 43 of the GDPR, the EDPB explains: *"whenever the controller is a public authority, there is often a clear imbalance of power in the relationship between the controller and the data subject. It is also clear in most cases that the data subject will have no realistic alternatives to accepting the processing (terms) of this controller. The EDPB considers that there are other lawful bases that are, in principle, more appropriate to the activity of public authorities."*[223]

A third argument why consent is not a possible legal ground for most data processing through the use of Meetings, is that the Content Data may contain personal data from other employees or other data subjects who may have to provide personal data to create a guest account, or whose data are part of 'contacts' imported by an Enterprise or Education end user in their Zoom account. Universities and government organisations are not able to invite these other individuals to provide valid consent to Zoom for the processing of their personal data as part of the Content Data.

Zoom and the universities and government organisations can only rely on the legal ground of consent for the processing of some Content and Account Data for three purposes:

1. (For admins) Subscribe to mailing lists with announcements related to software updates, upgrades, and system enhancements,

2. (For end users) Make choices with regard to a screen name, profile picture and background, if the organisation does not prescribe the contents of these elements (such as a branded background),

3. Provide Feedback to Zoom, without being pushed or nudged, by actively looking up this option in the settings menu or on Zoom's public website.

To avoid misunderstandings, Zoom commits in the DPA never to directly ask for consent from end users for new types of data processing. It can only ask admins to opt-in to (actively enable) such new purposes. Zoom writes: "*Zoom shall not ask for Consent from End Users for new types of data processing, and shall not process Customer Personal Data for any "further" or "compatible" purposes (within the meaning of Articles 5(1)(b) and 6(4) GDPR) other than those specified in this Addendum or enabled by the Account Administrator.*"[224]

[222] Recital 49 of the GDPR: "*In order to ensure that consent is freely given, consent should not provide a valid legal ground for the processing of personal data in a specific case* ***where there is a clear imbalance between the data subject and the controller****, in particular where the controller is a public authority and it is therefore unlikely that consent was freely given in all the circumstances of that specific situation.*"

[223] EDPB, *Guidelines on consent*, paragraph 3.1.1.

[224] Zoom new DPA, Clause. 2.6.

12.1.2. Contract

Article 6 (1) (b) GDPR reads: "processing is **necessary for the performance of a contract** to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract."

When an organisation provides its employees with a paid Zoom account, it is plausible that the use of the tool is necessary to carry out the tasks included in the employees' job description or to study. Access to a videoconferencing service has become essential to work, teach and study from home. As described in section 7.1 of this report, it is plausible that even after the pandemic has subsided, universities and government organisations continue to have a strong interest in effective online teleworking. Use of Zoom enables universities to expand collaborations between universities, engage in new partnerships with companies, and collaborate with different government organisations, both nationally and internationally. Employees and students should be able to remotely organise meetings with people within the organisation and with external participants, share files and chat from multiple locations, and on different devices.

To the extent that the processing of the Content, Account, Diagnostic, Support and (logged-in) Website Data is strictly necessary for the performance of the (labour) contract which the data subject has with the government organisation or university, the organisation can successfully invoke this legal ground (not Zoom, as Zoom does not have a contract with each end user). This legal ground can only apply if the organisation requires employees and students to use Zoom Meetings to do their work or attend virtual classes, and there are no alternatives available. If there are alternatives, this legal ground is not adequate, as this legal ground can only be invoked if the data processing is strictly necessary for each individual end user.

Generally, universities and government organisations also use the videoconferencing software to communicate with other data subjects (not employees or students at the same university). Therefore, two other legal grounds need to be considered. These are: (i) the performance of a task carried out in the public interest (Article 6(1) e of the GDPR) and (ii) necessity for the purposes of their legitimate interests (Article 6(1)(f) of the GDPR).

12.1.3. Public interest and legitimate interest

Article 6 (1) (e) GDPR reads: "processing is **necessary for the performance of a task carried out in the public interest** or in the exercise of official authority vested in the controller."

Article 6 (1) (f) GDPR reads: "processing is **necessary for the purposes of the legitimate interests** pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child**.**"

The last sentence of Article 6(1) of the GDPR adds: "Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks."

The last sentence of Article 6(1) of the GDPR excludes the application of the legitimate interest ground for processing carried out by public authorities in the performance of their tasks. However, the choice to use certain videoconferencing software is secondary to the performance of public tasks by public authorities, and can therefore also be considered as a task primarily exercised under private law.

As explained in Recital 47 of the GDPR, the legal ground of necessity for the legitimate interest (Article 6(1) f) is more likely to exist *where there is a relevant and appropriate relationship between the data subject and the controller in situations such as where the data subject is a client or in the service of the controller.*

When Zoom Meetings is used to communicate with external data subjects (guest users with a paid or free Zoom account) for the performance of public tasks, or the use is mandatory to follow classes for students, government organisations and universities may also invoke the legal ground of the performance of their public tasks.[225]

Both legal grounds require an assessment of the necessity of the personal data processing, of the proportionality and availability of alternative, less infringing means to achieve the same legitimate purposes (subsidiarity).

Initially, Zoom shared Website Data with third parties that are independent data controllers and could process the data for their own marketing purposes. These companies were not contracted as subprocessors by Zoom. As a result of the discussions with Zoom and repeat inspections of the website traffic, in February 2022 Zoom changed the default settings to 'strictly necessary', and removed traffic to and from third parties at the default level.

Zoom also disabled by default other types of data processing for EU customers (such as the Feedback functionality). As described in Section 4.2, Zoom offers extensive controls for admins to enable E2ee and block some functionalities for all end users if they assess the resulting data processing could be harmful to some participants, depending on the type of organisation and characteristics of the participants, such as age.

When Dutch universities and government organisations sign the new DPA, and carefully consider the most privacy friendly settings to protect the rights of all Meetings participants, they can successfully appeal to the legal ground of necessity for their legitimate interest for all data processing by Zoom as a data processor when contract, consent or necessity for a task carried out in the public interest do not apply.

12.2. Zoom as data controller

As discussed in Section 6.3, Zoom as a data controller can legitimately process some (limited) personal data for its own business purposes, when the processing is necessary. The universities and government organisations explicitly authorise Zoom in the new DPA to 'further' process some personal data for Zoom's own legitimate business purposes.

The six authorised purposes (as summarised in Section 6.3 of this report) are:

1. billing, account, and customer relationship management,
2. complying with, and resolving legal obligations (including CSAM scanning),
3. abuse and virus detection, prevention, and protection,

[225] In the Netherlands, Chapter 7 of the law on higher education and scientific research (Wet Hoger Onderwijs en wetenschappelijk onderzoek contains the legal conditions for education on which the use of Zoom may be based as necessary processing in the public interest.

4. Using pseudonymised and/or aggregated data to improve and optimize the performance and core functionality of the Services,

5. Using pseudonymised and/or aggregated data for internal (financial) reporting and planning,

6. Using pseudonymised and/or aggregated data from Feedback for Zoom's overall service improvement.[226]

As Zoom is prohibited from asking end users for consent (except for cookies that are not strictly necessary), does not have a contract with individual users or account holders, and is not a public sector organisation, the only applicable legal ground for Zoom as a data controller is the necessity for its legitimate business interest.

12.2.1. Necessity for Zoom's legitimate interest

When drafting these six purposes in the DPA, a compatibility test was performed by SURF and Zoom, as required in Art. 6 (4) of the GDPR. This test consists of (at least) five steps. In abbreviated format:

1. the link between the collection and the further processing,

2. the relationship between the end users and Zoom,

3. the sensitivity of the data,

4. the possible consequences of the processing, and

5. the existence of appropriate safeguards such as encryption or pseudonymisation.

The DPA stipulates that processing for all six purposes is only permitted when strictly necessary and proportionate. This principle puts an obligation on Zoom to assess if it can use less data or less sensitive to achieve the same purpose (*data minimisation*).

For the first purpose, Zoom can legitimately process some Diagnostic Data for billing and account management, and contact data from its commercial sales contacts at Dutch government organisations and universities for its own legitimate business interest, as an independent data controller. As long as Zoom continues to offer an opt-out in every e-mail, and does not share personal data with third parties, Zoom can rely on the legal ground of Art. 6 (1) f of the GDPR to inform its contacts about new products, events or business propositions.

Similarly, Zoom has a legitimate business interest to process personal data about its website visitors, as long as it only sets and reads strictly necessary cookies, and asks for clear consent for any other type of information exchange or data transfer to the USA. Organisations can use a Vanity URL to allow end users to sign-in without having to visit Zoom's public website.

Both types of data processing do not involve any sensitive data, are predictable for the data subjects (*surprise minimisation*) and cannot lead to any grave consequences for the end users.

[226] Zoom new DPA, Clause 2.4.

The second purpose, of complying with legal obligations, can only pass the compatibility test because of four safeguards that outweigh the possible grave consequences for data subjects and the sensitive nature of Content Data. These are:

1. The application of E2EE to the Meetings and to chats (Advanced Chat),

2. The pseudonymised nature of most of the Diagnostic and Support Data. Additionally, organisations can pseudonymise the Account Data by using SSO. As an additional safeguard against the new US fiscal obligation to retain IP addresses of end users for 3 to 6 years, Zoom has committed to work on a solution to prevent identifiability of these IP addresses.

3. The retention period of maximum 12 months for Diagnostic and Support Data

4. Zoom's commitment to comply with the five conditions for disclosure (see Section 6.3.1), including the commitment to legally fight every order (with or without a non-disclosure order) specifically aimed at EU Enterprise or Education customers, and its public lobby to reform US surveillance law.

Based on these guarantees, Zoom can rely on the ground of the necessity for its legitimate business from a GDPR-perspective, in combination with its legal obligations under US law to comply with orders, warrants and subpoenas, when Zoom is compelled to disclose personal data to law enforcement and security services.

The third purpose, of enforcing its acceptable use policy, includes proactive scanning for illegal Child Sexual Abuse Material with Microsoft's PhotoDNA and forwarding of matches to the US NGO NCMEC. Similar to the second purpose, this similarly potentially involves grave consequences for data subjects and highly sensitive data (a possible flag as a person involved with CSAM).

Based on the confidentiality requirements of the ePrivacy Directive, the scanning of content for this purpose is prohibited. As explained in Section 10, electronic communication providers such as Zoom have to comply with these rules since the end of December 2020, when the European Electronic Communications Code entered into force.

There has been a heated debate in the EU about possible ad hoc measures legitimising child abuse detection activities by electronic communication providers. On 6 July 2021, the European Parliament accepted a temporary derogation from the ePrivacy rules to allow providers of electronic communication service providers (such as Zoom) to detect remove and report child sexual abuse online for a period of three years.[227]

The draft measure is public, but no applicable law yet: it first has to be approved by the European Parliament. After that, the Council will immediately adopt the measure. In an initial analysis of the proposal, the EDPS (the data protection authority supervising the European institutions) warned against the interference with the fundamental rights to respect for private life and data protection of all users of very popular electronic communications services. Even voluntary measures by private companies constitute an interference with these rights, the EDPS explained. The proposal for

[227] Portuguese EU Presidency, Combating child abuse online – informal deal with European Parliament on temporary rules, 29 April 2021, URL: https://www.2021portugal.eu/en/news/combating-child-abuse-online-informal-deal-with-european-parliament-on-temporary-rules/. Text adopted by the European Parliament on 6 July 2021, URL: https://www.europarl.europa.eu/doceo/document/TA-9-2021-0319_EN.html.

mandatory prior guidance by data protection authorities cannot substitute compliance with the requirement of legality and thirdly, the legislation must be detailed and precise enough to guard the proportionality of the processing.

Zoom has taken technical measures to make it nearly impossible to raise false alarms, by only reporting on exact matches with 'known' material. Zoom does not use AI to predict matches. Zoom also contractually guarantees to conduct a human review before the data are shared with NCMEC. The scanning is applied to Zoom Room backgrounds and avatars, and only to persistent chat file uploads if the chat is not encrypted with the end user keys. If an end user account is terminated because of a (human-confirmed) match, the user will be enabled to file an appeal. Additionally, Zoom contractually commits to follow any future EDPB guidance with respect to this content scanning.

For the fourth and fifth purpose Zoom is not permitted to use directly identifiable data, but must aggregate. Zoom is specifically prohibited from aggregating on a per-Customer (per tenant) level. This agreed high level of aggregation is an important guarantee to protect the confidentiality of the use of Zoom services. As discussed in Section 5.2.2, Zoom is not allowed to perform types of analyses at an individual customer level, such as average time spent in Meetings per day of the week by users of a specific organisation. Within these confinements, Zoom can invoke its legitimate interest (and the interest of its customers) in using statistical data for purposes such as improving the services, internal reporting and capacity planning.

The sixth purpose, of aggregating Feedback Data, can easily be qualified as compatible, as the initial purpose of the processing is either based on individual free consent, or based on a compatibility assessment of the organisation that decides to enable this functionality. The 'further' processing of these data does not prevail over the rights and freedoms of the end users.

13. Special categories of data

Special categories of data are "*data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health, data concerning a natural person's sex life or sexual orientation* (Article 9 GDPR). In addition, Article 10 of the GDPR prohibits the processing of "*personal data relating to criminal convictions and offences or related security measures.*"

As explained in section 3.5.1 of this DPIA, it is up to the individual universities and government organisations to determine if they process special categories of data, in the contents of Meetings or recordings/transcriptions/chats stored locally or in Zoom's cloud.

Organisations must also consider the risk that special categories of personal data (or otherwise sensitive data) could end up in the metadata, such as

- user provided Room Names (in the test scenarios *sollicitatiegesprek F.Ictief*, *Inkoopgunning* and *Staatsgeheim*)
- user provided categorisations (in the test scenarios *boss*, *boring* and *sexy*)
- user provided tracking fields such as *HR*, or *Klantcontact*
- contents of user filed remote support request

user provided topic names (in the test scenarios, topic names were used such as *Sollicitatiegesprek* and *Inkoopgunning*)

These data may be stored in combination with usernames and email addresses (as Host, as participants in a chat or as attendees), if the organisation does not use SSO.

As discussed in Section 8, there are high data protection risks for end users if special categories of personal data would be forcibly disclosed by Zoom to law enforcement authorities and security services.

To prevent this high risk, organisations are advised to enable to encrypt Content Data with E2EE and Advanced Chat if they know that special categories of data are exchanged via Meetings. Additionally, to reduce the risk of mass surveillance of the other categories of personal data, Zoom has committed to develop primarily EU data processing options (for Support Data by mid-2022, for all other personal data by the end of 2022).

To further mitigate the risks relating to undue access to the metadata, universities and government organisations can create policy rules to prevent Zoom from processing confidential or sensitive data through the unencrypted metadata. They could for example draft a policy to prohibit the use of directly identifying personal or confidential data in room and topic names, in user categorisations and perhaps, in some circumstances, warn users about the risks of using profile pictures (for example, in contacts with external participants).

14. Purpose limitation

The principle of purpose limitation is that data may only be "*collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes*" (Article 5 (1) (b) GDPR). Essentially, this means that the controller must have a specified purpose for which he collects personal data, and can only process these data for purposes compatible with that original purpose.

Data controllers must be able to prove, based on Article 5(2) of the GDPR, that they comply with this principle (*accountability*). As explained in section 6.2 of this report only data controllers may take decisions about the purposes, including decisions about retention periods and transfers to third parties to process the data for additional purposes. As data processor, Zoom may not process the personal data for other than the five authorised purposes, plus the six additional purposes for which Zoom is authorised to 'further' process some personal data. As assessed in Section 12, Zoom and the universities/government organisations have a legal ground for each of the agreed 'processor' purposes, and the additional purposes meet the compatibility test of Art. 6 (4) of the GDPR. With Zoom's additional explanations (described in Section 5) the purposes comply with the requirement of *surprise minimisation.* As quoted in Section 5.2.2, Zoom has a policy and processual rules to ensure security and privacy officials sign off on proposed new data processing before it can be entered in production. At the request of SURF, Zoom will have its compliance with purpose limitation verified in a SOC-2 audit.

The principle of purpose limitation is inextricably linked to *transparency* requirements. A data controller must have a limitative overview of the categories of personal data that may be processed

for each distinct purpose. As a result of the discussions with SURF, Zoom has developed a new Data Privacy Sheet, with detailed, event level descriptions of the different Diagnostic Data it collects (the Meeting Metadata, the Telemetry Data and the Service Generated Data). See Section 15.2 below.

In sum, thanks to Zoom's many improvement measures, and the new DPA with a limitative list of specific purposes, Zoom's customers should be able to rely on the contractual guarantees and privacy controls to prevent any personal data from being processed beyond these authorised purposes.

15. Necessity and proportionality

15.1. The principle of proportionality

The concept of necessity is made up of two related principles, namely proportionality and subsidiarity. Personal data that are processed must be necessary for the purpose pursued by the processing activity. Proportionality means the invasion of privacy and the protection of the personal data of the data subjects is proportionate to the purposes of the processing. Subsidiarity means that the purposes of the processing cannot reasonably be achieved with other, less invasive means. If so, these alternatives have to be used.

Proportionality demands a balancing act between the interests of the data subject and the data controller. Proportionate data processing means that the amount of data processed is not excessive in relation to the purpose of the processing. If the purpose can be achieved by processing fewer personal data, then the data controller needs to limit the processing to personal data that are necessary.

Therefore, data controllers may only process personal data that are necessary to achieve legitimate purpose. The application of the principle of proportionality is thus closely related to the principles of data protection from Article 5 GDPR.

15.2. Assessment of the proportionality

The key questions are: are the interests properly balanced? And does the processing not go further than what is necessary?

To assess whether the processing is proportionate to the interests pursued by the data controller(s), the processing must first meet the principles of Article 5 of the GDPR. As legal conditions they have to be complied with in order to make the data protection legitimate.

Data must be '*processed lawfully, fairly and in a transparent manner in relation to the data subject*' (Article 5 (1) (a) GDPR). This means that data subjects must be informed about the processing of their data, that all the legal conditions for data processing are adhered to, and that the principle of proportionality is respected. As analysed in Sections 12.1 and 12.2 of this report, due to Zoom's many improvement measures, the universities and government organisations have a legal ground for all data processing through Zoom Meetings. Where they authorise Zoom to 'further' process some personal data for specific purposes, Zoom has a legal ground. This means the personal data are processed lawfully.

Another important result of the dialogue with SURF after the first DPIA is that Zoom has thoroughly complied with its transparency obligations. In its new Data Privacy Sheet, Zoom publishes information

about the contents and purposes of the different kinds of Content Data, the different kinds of Account Data, Diagnostic Data, Website Data, Support Data and Feedback/Marketplace Data.[228] In its new Cookie Policy, Zoom informs its website visitors about the different categories of cookies, the purposes and the default settings, with a hyperlink to the more detailed information in its Cookie Consent manager.[229] Last but not least, Zoom has revised its data retention policy. As detailed in Table 5, Zoom clearly defines the (new) retention periods for each category of personal data in the DPA agreed with SURF and HEAnet.

As part of its transparency commitments, Zoom has committed to improve access to individual personal data, by developing three new take-out tools by the end of 2022. These are: (i) an improved take-out for admins of all personal data relating to a specific data subject, (ii) a self-service take out for data subjects to file Data Subject Access Requests, and (iii) a take-out of admin behaviour (to check administrator compliance with policy rules). These take-outs compensate for the fact that there is no easy access to the Telemetry Data and Webserver access logs, nor a complete overview of personal data in system generated server logs. Previously, the lack of transparency made the data processing inherently unfair. The lack of transparency also made it impossible to assess the proportionality of the processing. Based on the measures already taken and agreed to, Zoom has convincingly solved these initial shortcomings.

The principles of data minimisation and privacy by design require that the processing of personal data be limited to what is necessary: the data must be "*adequate, relevant and limited to what is necessary for the purposes for which they are processed*" (Article 5(1)(c) of the GDPR).' This means that the controller may not collect and store data that are not directly related to a legitimate purpose.

The principle of privacy by design (Article 25 (2) GDPR) requires that "*the data controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. According to this principle, the default settings for the data collection should be set in such a way as to minimise data collection by using the most privacy friendly settings.*"

As described in Section 9.3 of this report, Zoom already processed personal data with privacy friendly default settings for admins and for end users, but has agreed to further minimise the data processing to the extent strictly necessary to provide the contracted services. This includes minimisation of information collected via cookies on its Website, and minimisation of data retention periods. Zoom also contractually agrees to perform a DPIA before introducing new features or related software and services.

Zoom notably failed to apply the principle of privacy by design with regard to the processing of Website Data. In its consent manager, the default setting on the publicly accessible web pages was to accept third party tracking cookies. After some retesting, Zoom's website was found to comply with both the ePrivacy and GDPR transparency and consent requirements. European Education and Enterprise customers can also use their own vanity subdomain, where they are in full control over the use of cookies.

As discussed in Section 12.2.1, the proactive scanning of Content Data for CSAM, and forwarding of matches to an US NGO, is a high-risk type of data processing. A match may have grave consequences for data subjects, if they are flagged as a person involved with CSAM, and their account is suspended.

[228] Zoom Privacy Data Sheet, URL: https://explore.zoom.us/media/privacy-data-sheet-feb.pdf.

[229] Zoom Cookie Statement, URL: https://explore.zoom.us/en/cookie-policy/.

Zoom has taken technical measures to minimise the chances of false positives, and only scans limited data, not the streaming data.

The principle of storage limitation requires that personal data should only be kept for as long as necessary for the purpose for which the data are processed. Data must *'not be kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the personal data are processed*' (Article 5(1)(e), first sentence, GDPR). This principle therefore requires that personal data be deleted as soon as they are no longer necessary to achieve the purpose pursued by the controller. The text of this provision further clarifies that *'personal data may be kept longer in so far as the personal data are processed solely for archiving purposes in the public interest, for scientific or historical research purposes or for statistical purposes in accordance with Article 89(1), subject to the implementation of appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject*' (Article 5(1)(e), second sentence, GDPR).

As explained in Section 11 of this report, Zoom will generally retain personal data for a maximum of 12 months, or, as long as the contract lasts with the end user or the government organisation or university, plus a back-up of 35 days. Additionally, Zoom retains files and images exchanged in both recorded and unrecorded meetings for 24 hours after the meeting and retains cloud recording raw files for 15 days after the customer initiated the recording. With this data retention policy Zoom's processing meets the proportionality requirements.

New US Treasury rules require service providers that wish to benefit from tax deduction to provide evidence that income is not earned in the USA. This would require retention of the IP addresses for a period of 6 years. Zoom has committed to actively explore alternative routes to providing sufficient evidence without retaining identifiable IP addresses.

15.3. Assessment of subsidiarity

When making an assessment of subsidiarity, the key question is whether government organisations and universities can reach the same objectives (of using secure, bug free, modern videoconferencing, chat and file exchange software), with less intrusive means.

Universities and government organisations can choose alternative providers of videoconferencing tools. Many already use Microsoft Teams as an alternative, but they should also consider the use of open-source software such as Jitsi, Nextcloud Talk, BigBlueButton or BlueJeans. Such an assessment is urgent, in view of the recent enforcement actions by different national supervisory authorities (DPAs) on transfers of personal data to the USA, including IP addresses transferred to Google for website analytics, or to access remotely hosted fonts used on a website.

SLM Rijk has published several DPIAs on Microsoft 365 and both the Dutch government and SURF have centrally negotiated GDPR-compliant privacy conditions. Regardless of a choice for an alternative software provider, organisations must identify the privacy and security risks of any software or cloud service they plan to use, and assess whether the software offers the necessary functionalities.

16. Data Subject Rights

This Section assesses whether universities/government organisations and Zoom meet the GDPR requirements relating to data subjects rights and whether data subjects can effectively exercise such

rights. Section 16.1 discusses the applicable GDPR framework and the arrangements in place between Zoom and its Education and Enterprise customers in the EU. Sections 16.2 to 16.7 analyse whether data subjects can effectively exercise each of these rights.

16.1. Legal framework and contractual arrangements

The GDPR grants data subjects the right to information, access, rectification and erasure, object to profiling, data portability and file a complaint. It is the data controller's obligation to provide information and to duly and timely address these requests. If the data controller has engaged a data processor, the GDPR requires the data processing agreement to include that the data processor will assist the data controller in complying with data subject rights requests. In the event of joint controllership, the GDPR requires that the joint controllers 'shall in a transparent manner determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the exercising of the rights of the data subject and their respective duties to provide the information referred to in Articles 13 and 14, by means of an arrangement between them'. The essence of the arrangement shall be made available to the data subjects.

16.2. Right to information

Data subjects have a right to receive easily accessible, comprehensible and concise information about the processing of their personal data. This means that data controllers must provide data subjects with, inter alia, their identity as data controller, the purposes of the data processing, the intended duration of data storage and the data subjects' rights under the GDPR.

As assessed in Section 15.2, as a result of the dialogue with SURF, Zoom has decided to provide its customers and end users with comprehensible new information about the processing of personal data, through its new Data Privacy Sheet and Cookie Policy. This includes detailed, event level information about the three different kinds of Diagnostic Data. Based on this information, organisations can provide data subjects adequate information about the processing of their personal data, Zoom's identity as a data processor, the intended duration of the storage and how data subjects can exercise their rights.

16.3. Right to access

Data subjects have a right to access their personal data. Upon request, data controllers must inform data subjects whether they are processing personal data about them. If this is the case, data subjects should be provided with a copy of such personal data, together with information about the purposes of processing, recipients to whom the data have been transmitted, the retention period(s), and information about their further rights as data subjects, such as filing a complaint with a Data Protection Authority.

Zoom stipulates in its DPA that its customers are primarily responsible for responding to Data Subject Requests. In other words, end users must turn to their admins for all data subject requests. When Zoom is a data controller, Zoom will answer such requests.

"*Zoom will advise the Data Subject to submit their request to Customer and Customer will be responsible for responding to such request, including, where necessary, by using the functionality of the Services.*

Zoom shall, taking into account the nature of the Processing, assist the Customer by appropriate technical and organizational measures, as far as this is possible, for the fulfilment of the Customer's

obligation to respond to requests for exercising the Data Subject's rights (regarding information, access, rectification and erasure, restriction of Processing, notification, data portability, objection and automated decision-making) under Applicable Data Protection Law." [230]

As described in Section 3.1, Zoom provides administrators access to eight reports about usage activities and audit log files. These reports and log files do not provide a complete overview of all personal data processed by Zoom about the use of Zoom Meetings. Zoom also does not yet provide (automated) access to the website and cookie data it collects on its restricted access and publicly accessible website, or other data such as Support Data, nor to the raw data collected by Zoom about Feedback/Marketplace. Zoom initially failed to provide information in request to two DSARs. Zoom only referred to the information available in-product for users and in the console for Zoom admins. However, in a second, more extensive reply, Zoom provided information from its three kinds of server logs (Meeting Logs, Event Logs (with the Telemetry Data) and Account Logs), and some Website Data.

In reply to the first DPIA, Zoom has committed to manually assist admins with full access to all available personal data, until the three new take-out tools are ready (by the end of 2022). This should include access to identifiable data from its public and restricted access Website request logs. Zoom can only rely on the exception in Article 11(2) of the GDPR on access requests that it is unable to identify the data subject after it has accepted offers from the requesting data subjects to receive additional information enabling their identification.

Now that Zoom has changed its cookie policy, and by default only sets and reads strictly necessary first party cookies on its website for EU visitors, it no longer automatically transfers personal data to third parties via cookies, and does not need to include these data in a data subject access request, unless the visitor has consented to such processing.

16.4. Right of rectification and erasure

Data subjects have the right to have inaccurate or outdated personal data corrected, incomplete personal data completed and - under certain circumstances - personal data deleted or the processing of personal data restricted. End users can erase the data they have uploaded to their profile, such as a screen name, profile picture, and imported contacts and calendar data. Admins of government organisations and universities can delete individual end user accounts, but this does not yet result in automatic deletion of historical metadata relating to that end user.

As described in Section 11, Zoom applies different retention periods to the content and metadata. Most personal data are retained for 12 months from the date of collection. Zoom has shorter retention periods for files and images transferred during a meeting (24 hours retention) and raw cloud recording files (15 day retention from date of recording). Additionally, Zoom will retain limited information (Account Data and cloud recordings) for the life of the account, plus 35 days backup.

Based on the requirements of Article 17(1)(a) and Article 17(1)(d) of the GDPR, universities and government organisations must be able to delete personal data without undue delay upon request of a data subject if they are no longer needed for the purposes for which they were collected or otherwise processed, or when the personal data have been unlawfully processed. Zoom has contractually agreed in the DPA to support its EU customers to comply with this obligation, and will develop an individual data deletion tool before the end of 2022.

[230] Zoom new DPA, Clauses 8.1 and 8.2.

16.5. Rights to object against direct marketing and profiling

Data subjects have the right to object against the processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing. (Article 21 (2) GDPR).

Data subjects have "*the right not to be subjected to an exclusively automated decision if it has legal effects, including profiling.*" (Article 22 (1) GDPR).

In the new DPA, Zoom is specifically prohibited from processing any personal data for marketing or profiling purposes, unless the end user has subscribed to a mailing list, or in relation to Zoom's commercial contacts (the Account Holders, such as procurement officials and sales managers).

"*Zoom will not Process Customer Personal Data for advertising purposes or serve advertising in the Services and Zoom will not process Customer Personal Data for direct marketing, profiling, research or analytics purposes except where such processing is necessary (i) to comply with Customer's instructions as set out in Section 2.2 of this DPA or (ii), only for the purposes of reporting, planning, modelling and analytics, in accordance with the Legitimate Business Purposes described in Section 2.4.*"[231]

This prohibition also extends to guest users. Even when they participate in a Meeting hosted by an EU Enterprise or Education customer with a 'free' account, which can include advertising[232], Zoom is prohibited from using any information about such meetings for its consumer advertising. Hence, Zoom will not show an advertisement to these users at the end of meetings.

To further assist data subjects with their absolute right to object to direct marketing, Zoom has committed to develop a self-service marketing preference tool by the end of 2022. This will enable everybody, including Zoom's commercial contacts, to subscribe or unsubscribe from different mailing lists.

Possible profiling

With regard to profiling, Zoom is required based on US law to scan some Content Data for child abuse material. Since 6 July 2021, such data processing is permitted in the EU, based on a temporary derogation of the ePrivacy rules.

As analysed in Section 12.2.1 and 15.2, Zoom has taken steps to ensure its legitimate interest in complying with these requirements does not outweigh the data subjects' rights to protection of their private life and personal data. Zoom additionally commits in the DPA to comply with any future guidance from the EDPB relating to this data processing:

"*With regard to content scanning for Child Sexual Abuse Material ("CSAM") and reporting 'hits' to The National Center for Missing & Exploited Children ("NCMEC"), Zoom shall comply with applicable regulatory guidance from the European Data Protection Board ("EDPB"). Zoom will conduct human review of matched content before it is reported. Zoom will immediately suspend the account of the end user, but will notify the end user of the suspension and the possibility to appeal to this decision.*"[233]

[231] Zoom new DPA, Clause. 2.5.

[232] Zoom, Zoom Supports Continued Access for Basic Users with Advertising Program, 1 November 2021, URL: https://blog.zoom.us/zoom-continued-access-for-basic-users-with-advertising-program/.

[233] Zoom new DPA, Clause. 2.7.

16.6. Right to data portability

Data subjects have a right to data portability if the processing of their personal data is carried out by automated means and is based on their consent or on the necessity for the performance of a contract. As explained in Sections 12.1 and 12.2 of this report, consent can only be provided by end users for very limited data processing, while the processing by the Dutch government organisations/universities can be based on the necessity to perform the (labour) contract, but this may not always be the case. If so, Zoom needs to assist it customers to help them with data portability requests from its employees and students.

16.7. Right to file a complaint

Finally, as data controllers universities and government organisations must inform their employees and students about their right to complain, internally to their Data Protection Officer (DPO), and externally, to the Dutch Data Protection Authority (Autoriteit Persoonsgegevens). The contact details are included in the SCC that form part of the new DPA.

In sum, Zoom and its customers (the universities and government organisations) have agreed on measures to (fully) honour the rights of data subjects.

Part C. Discussion and Assessment of the Risks

17. Risks

17.1. Identification of risks

The processing of personal data in and about Zoom Meetings results in two types of general risks. First, risks through the processing of Diagnostic Data, Support Data, Website Data and Feedback/Marketplace Data about the use of the services and secondly, risks resulting from the processing of Content Data, including the Account Data.

17.1.1. Metadata

As explained in Section 1.2, use of the Zoom Meeting services results in the processing of different types of Diagnostic, Support, Website and Feedback Data.

Zoom qualifies itself as the data processor for all personal data, except for the public Website Data. As analysed in Section 14 (Proportionality) Zoom may only process these metadata for limited purposes, when strictly necessary and proportionate. Zoom has subprocessor agreements with the third parties it engages, and has inventoried the subprocessors' subprocessors. All subprocessors are contractually bound to the same privacy conditions agreed with its EU Education and Enterprise customers. As a result of the negotiations with SURF, Zoom has become as processor, agreed to purpose limitation, greatly enhanced transparency and committed to develop additional guarantees. These measures ensure that the data protection risks for end users are limited.

A different category of risks results from the processing of the metadata by the admins of the EU Education and Enterprise customers. They have access to audit log files and reports with information about individual user activities. Universities and government organisations could potentially combine information from these log files to create a (performance) profile of Zoom end users. Universities and government organisations can mitigate these risks by adopting clear policy rules to prevent the use of the log files for employee evaluation purposes. As soon as Zoom offers an easier auditing of admin behaviour, organisations can use these logs to verify that the logs are not misused for unauthorised purposes.

17.1.2. Content Data

Zoom collects and processes content included in Content Data in different ways. For example, Zoom processes the live video, audio and text streams, stores exchanged files, and can also store transcriptions and recordings of the meetings and chats on its cloud servers. Content Data may also be included in Support Data and in text entered in the open text input in the Feedback form. End users can provide Content Data to Zoom in the context of their Zoom Account, such as their screen name, profile pictures, and imported contacts and calendar data.

As explained in Section 3.5.1 of this report, the Content Data may include sensitive or confidential information, and sensitive and special categories of personal data relating to many categories of data subjects, not just employees and students. It is likely that many government and university employees will process personal data of a sensitive nature by using Zoom Meetings. For example, employees may discuss sensitive financial data in relation to subsidies, or exchange files with data about crimes or

convictions. Such personal data of a sensitive nature can be stored on Zoom's cloud servers, if not prohibited by admins, also as transcripts of conversations or chat histories. If Meeting hosts use special categories of data as room or meeting names, or qualify guest attendees with categorisations about their health (for example: blind, audio only), such qualifications can become part of the Diagnostic Data.

Even though Zoom already exclusively processes streaming data of its EU customers in data centres in the EU, access to these data can be ordered through US legislation such as the US CLOUD Act. Following the Schrems-II ruling from the European Court of Justice and the guidance from the EDPB and the EDPS on measures and guarantees to protect the data against mass surveillance in the USA, the only adequate technical measure is the application of E2EE. Zoom offers this protection for all streaming data and chats. Additionally, Zoom has committed to develop an exclusive EU cloud by the end of 2022 for its EU Education and Enterprise customers, for all personal data processing. The only exception is the ongoing access by the Trust & Safety Team in the USA to other service generated server logs, in order to attach a pseudonymised identifier to recognise and ban individuals that have been marked as bad actors.

17.2. Assessment of Risks

The risks can be grouped in the following categories:

- Inability to exercise rights (including but not limited to privacy rights);
- inability to access services or opportunities;
- loss of control over the use of personal data;
- discrimination;
- identity theft or fraud;
- financial loss;
- reputational damage;
- physical harm;
- loss of confidentiality;
- re-identification of pseudonymised data; or
- any other significant economic or social disadvantage[234]

These risks have to be assessed against the likelihood of the occurrence of these risks and the severity of the impact.

The UK data protection commission ICO provides the following guidance: "*Harm does not have to be inevitable to qualify as a risk or a high risk. It must be more than remote, but any significant possibility of very serious harm may still be enough to qualify as a high risk. Equally, a high probability of widespread but more minor harm might still count as high risk.*"[235]

[234] List provided by the ICO, How do we do a DPIA, Step 5: How do we identify and assess risks?, URL: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/how-do-we-do-a-dpia/.

[235] Idem.

In order to weigh the severity of the impact, and the likelihood of the harm for these generic risks, this report combines a list of specific risks with specific circumstances of the specific investigated data processing.

17.2.1. Loss of control, loss of confidentiality: undue access by US government authorities to Content Data

Zoom offers a possibility to apply E2EE to Meetings and chats, including exchanged files. This means that even if Zoom is compelled to intercept these data, it cannot lift the encryption. Only end users have access to the encryption keys. When E2EE and Advanced Chat encryption are enabled, organisations cannot use Zoom's cloud recordings and transcriptions. They can however choose to deploy local recording, and apply their own encryption keys to such local storage.

With cloud recording, Zoom applies the encryption and has access to the keys. Hence, if an organisation does not use E2EE and uses Zoom's cloud recording, there is a chance that US law enforcement, courts or secret services may compel Zoom to lift its own encryption and disclose these data in decrypted format. As shown in the DTIA performed as part of this DPIA, the likelihood that this risk will manifest is very slim, based on historical experience and a comparison with other cloud providers. Even if the likelihood of occurrence is extremely low, the impact on data subjects in case of disclosure of their personal data to US law enforcement or security services can be extremely high. This is due to the lack of notification and the lack of an effective means of redress for EU citizens. This risk even occurs in the current circumstance that the cloud recordings and recorded chats are exclusively processed and stored in data centres in the EU, because access to these stored data can be ordered through US legislation such as the US CLOUD Act.

By applying E2EE, Advanced Chat encryption and using local recording, organisations can effectively limit the impact of undue access to the streaming Content Data to zero, regardless of the nature of the data. Therefore, organisations can use Zoom Meetings to exchange even sensitive and special categories of data, with a low risk for data subjects.

This assessment comes with a **caveat**. Organisations are advised to take heed of a possible different explanation in the future risk assessment by the EDPS and the EDPB, as a result of the taskforce public sector use of Cloud Providers.

17.2.2. Loss of control: undue access by US government authorities to Diagnostic, Support and Website Data

As described in Section 8.1, Zoom systematically transfers all personal data but the streaming Content Data to the USA, a country without adequate data protection rules.

It follows from the risk calculation in the DTIA that the likelihood is very small that Zoom will be compelled to disclose these data to US government authorities. These risks can be accepted, as these risks will be largely mitigated by the end of 2022 the latest, after completion of Zoom's EU Cloud. This enables EU Education and Enterprise customers to ask Zoom to collect, process and store the Content Data, the Diagnostic Data, as well as the Account Data and the Support Data, in Zoom's EU data centres.

To further mitigate some of the risks of compelled disclosure to USA government authorities, universities and government organisations can create policy rules to prevent Zoom from processing sensitive or special categories of data through the Diagnostic Data. It is up to the government

organisations and universities to determine what risks they consider acceptable related to the transfer of personal data to the USA. Depending on the sensitivity and confidentiality of the data, they may want to apply additional data minimisation measures, such as using Single Sign On to provide Zoom with pseudonyms, and ensuring through conditional access that guest users accept the organisation's privacy conditions.

Zoom's contractual promises to legally resist all orders that are specifically targeted at EU Enterprise and Education customers, its transparency reporting, minimised data retention periods and the announcement of an exclusive EU cloud for all personal data by the end of 2022, make the likelihood of the occurrence of undue access by US law enforcement agencies to these personal data very low. Therefore, the risks for data subjects can be qualified as low. This of course provided the organisations and universities apply the recommended data minimisation measures.

17.2.3. Loss of control and reidentification: undue access by US government authorities to pseudonymised Diagnostic Data (ongoing)

After 2022, Zoom will continue to systematically transfer pseudonymised Diagnostic Data to its central Trust & Safety Team in the USA, to identify and block bad actors that threaten the security and integrity of Zoom Services. This data is accessible only by Zoom employees with a need to know and subject to appropriate technical and organisational measures. This transfer should only involve pseudonymous identifiers, no Content Data or usernames.

In view of the legitimate purpose of the processing, to recognise and mitigate security risks for all other end users and customers, it is necessary for Zoom to reidentify specific users based on their pseudonymous identifiers. It is plausible that Zoom needs to operate a central Trust & Safety team, and cannot perform these tasks in separate regionalised security teams, as bad actors may be located anywhere in the world.

As shown in the DTIA, the likelihood of compelled disclosure to US government authorities is low. Even though the impact of undue access could be very high, the risks for data subjects can be qualified as low.

17.2.4. Lack of transparency Account and Diagnostic Data

Following the first DPIA in May 2021, Zoom has greatly improved its transparency about the different categories of personal data it collects, generates and processes in its new Data Privacy Sheet and new Cookie Policy. As documented in Table 5, Zoom has also documented the retention periods for the Diagnostic Data, and shortened the retention period to 12 months after collection.

Zoom has committed to gradually expand its documentation. For example, when this Update DPIA was finalised, Zoom documented 42 of the 49 unique telemetry events. Zoom has also agreed to publish more detailed information about the processing of personal data in its webserver logs.

Initially, Zoom stored the metadata for a period of 5 years. Due to Zoom's lack of transparency about its retention periods and the contents of the Diagnostic Data, there was a non-negligible chance of loss of confidentiality, re-identification of pseudonymised data and unlawful (further) processing. In view of the measures Zoom has already taken since May 2021, and Zoom's firm commitment to comply with all GDPR transparency requirements, the risk that Zoom engages in new undocumented data processing, is small. Therefore, the privacy risks for data subjects can be qualified as low.

17.2.5. Difficulty to exercise Data Subject Access Requests

In response to two DSARs from the test Zoom accounts, Zoom initially did not provide the requested overview of all personal data it processed, even though it considered itself to be a data controller at the time. In a second, more extensive reply to the DSARs, Zoom did provide more Diagnostic Data, including Telemetry Data.

However, Zoom did not provide any information from its Website access server logs or data collected by third parties through cookies and similar technologies, because Zoom claimed it was not able to identify the data subject. Zoom did not accept the offer from the researchers to receive additional information enabling their identification, including providing access to all recorded network traffic including all kinds of unique device identifiers.

As a result of the negotiations with SURF, Zoom has committed to develop two types of automated Data Subject Access Request tools (i) an export tool of individual personal data for Account administrators and (ii) a do-it-yourself take-out tool for individual end-users. As long as these tools are not available, Zoom has committed to manually assist admins with full access to all available personal data. This should include access to available identifiable data from its public and restricted access (signed in) Website request logs. Zoom can only rely on the exception in Article 11(2) of the GDPR on access requests that it is unable to identify the data subject if it accepts offers from the requesting data subjects to receive additional information enabling their identification. Now that Zoom has changed its cookie policy, and by default only sets and reads strictly necessary first party cookies on its Website for EU visitors, it no longer automatically transfers personal data to third parties via cookies, and does not need to include these data in a data subject access request, unless the visitor has consented to such processing

In view of these commitments and improvements, data subjects can exercise their fundamental privacy rights, even though it currently still requires manual work from both Zoom and the admins of the organisations. That is why the privacy risks for data subjects are low.

17.2.6. Employee monitoring system: chilling effect

Admins of universities and government organisations that use Zoom have access to audit log files and reports with information about individual user activities, such as the sign-in/sign-out logs with information about the sign-in and sign-out times per identifiable user (user email address). They can also access information about participation in meetings in the active hosts report, insights in inactivity of users in the inactive hosts report and information about scheduled participation in upcoming events. Admins also have access to recorded chat histories if such chat histories are not end-to-end-encrypted with end user keys.

The audit logs could for example be used by the employer to reconstruct a pattern of the frequency and length of time spent in Zoom calls, with what other people. This is not easy. Zoom does not offer analytic tools for employers to easily create graphs and compare and assess work patterns of groups of employees. Zoom has even decided to remove a privacy invasive analytics tool to analyse attendee attention.[236] However, Zoom has committed to develop a tool to make it much easier for admins to take out all data relating to a specific user, in order to be able to answer Data Subject Access Request.

[236] Zoom, Attendee attention tracking, last updated 15 December 2021, URL: https://support.zoom.us/hc/en-us/articles/115000538083-Attendee-attention-tracking

Such a file could be used abusively, for a performance assessment, if use for such purposes is not specifically excluded in an (internal) privacy policy for the processing of employee personal data.

As a result of the Covid-pandemic, workers spend considerable amounts of work time using videoconferencing tools. That makes processing for such employee evaluation purposes more plausible. The knowledge that employers (universities and government organisations) can process the Diagnostic Data for profiling purposes can cause a *chilling effect* on employees and students of the Zoom Meeting services. A *chilling effect* is the feeling of pressure someone can experience through the monitoring of his or her behavioural data, discouraging this person from exercising their rights, such as accessing certain content.[237] Employees and students may feel unable to exercise their right to (moderately) make use of employer and study facilities without being observed and to communicate about private affairs, such as videoconferencing with a friend or family member. Employees may also feel unable to exercise their right to whistle blow, for example by organising a conference call with members of the Workers Council or Union.

Assuming the government organisations and universities follow the recommendations in this report to draft an internal ICT policy and verify compliance with this policy by regularly checking the admin logs, the risks for data subjects are low.

17.3. Summary of risks

These circumstances and considerations as explained above lead to the following six low data protection risks for data subjects:

1. Loss of control and loss of confidentiality: undue access by US government authorities to Content Data
2. Loss of control: undue access by US government authorities to Diagnostic, Support and Website Data
3. Loss of control and reidentification: undue access by US government authorities to pseudonymised Diagnostic Data (ongoing))
4. Lack of transparency Account and Diagnostic Data
5. Difficulty to exercise Data Subject Access Requests
6. Employee monitoring system: chilling effect

[237] Merriam-Webster Online Dictionary, "chilling effect", URL: https://www.merriam-webster.com/legal/chilling effect

Based on the ICO model, this results in the following matrix:[238]

Severity of impact	Serious harm	Low risk **1,2,3**	High risk	High risk
	Some impact	**Low risk 4,5,6**	**Medium risk**	**High risk**
	Minimal impact	**Low risk**	**Low risk**	**Low risk**
		Remote	Reasonable possibility	More likely than not
		Likelihood of harm (occurrence)		

[238] Copied from the DPIA guidance from the UK data protection commission, the ICO. URL: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/how-do-we-carry-out-a-dpia/.

Part D. Description of risk mitigating measures

Following the Dutch government's DPIA model, Part D describes the proposed countermeasures against the data protections risks identified in part C.

The following section contains a table of the mitigating technical, organisational and legal measures that can be taken by the universities/government organisations, and by Zoom.

18. Risk mitigating measures

Section 17.2 of this report describes six low privacy risks for data subjects. These risks can only be qualified as low as long as the universities and government organisations follow the recommended measures to mitigate some of these risks. The qualification as low risks is also dependent on Zoom's compliance with the measures it has committed to take.

Table 6 below shows the six low data protection risks for data subjects, with the mitigating measures government organisations, universities and Zoom must take.

Overview of six low risks and mitigating measures

No.	6 low risks	Measures gov orgs and universities	Measures Zoom
1.	Transfer of Content Data to the USA	Apply E2EE to all Meetings. Warn users that E2EE is not possible in browser	Comply with the SCC, inform SURF when compliance is no longer possible
		If E2EE is not applied: choose the EU as Content Storage Location setting. Consider local recording instead of cloud recording	
		Complete the model DTIA to assess the risks of unlawful access/disclosure of sensitive/ special/secret categories of personal data processed by Zoom	Do apply the contractually guaranteed human review after a match with known CSAM, allow end users to appeal to a decision to terminate their account
		Enable 'EU-only' for Support requests as soon as Zoom offers this option. Draft an instruction for admins when they can consent to export of Support data to third countries in exceptional circumstances	Organise an independent ISO and SOC-2 audit every year or two years: allow SURF and the central Dutch government to add one specific audit question every year
		Consider use of the available privacy options such as: • Enable advanced chat encryption • Prevent participants from saving chats • Mute individual or all participants upon entry • Turn off file transfer • Turn off annotation • Disable private chat • Turn off screen sharing for participants	Publish as much details as possible in the bi-annual transparency reports

		• Prohibit the (local) recording of video during screen sharing • Prohibit the viewing and recording of the 'gallery' during screen sharing	
		Only use Webinars for non-confidential, non-sensitive public data (no E2EE)	Update the DTIA if necessary, follow guidance from the EDPB
		Create policy rules to prohibit the use of directly identifying personal or confidential data in room and topic names. Do not use labels to categorise users. Perhaps, in some circumstances, instruct users not to use profile pictures	
2.	Transfer of Account, Diagnostic, Support and Website Data to the USA (until end of 2022)	Consider the use of SSO with pseudonymous identifiers for employees whose identity must remain confidential	Realise a general rule of personal data processing in the EU by the end of 2022, with known exception of the T&S Team.
			Update the DTIA if necessary, follow guidance from the EDPB
		Use a Vanity URL to prevent the transfer of IP addresses when end users sign in, and to prevent that end users visit Zoom's publicly accessible website hosted in the USA	Publish as much details as possible in the bi-annual transparency reports
		Do not use the default mail provider Twilio to send invitations for Webinars: use own EU-based mailing provider	Remove traffic to the US Consent Manager from the restricted access website located in the EU, to prevent transfer of personal data to the USA
3.	Transfer of pseudonymised Diagnostic Data to the USA Trust & Safety team (ongoing)	Follow guidance from SURF and the EDPB if this risk can be accepted, as calculated in the DTIA	Update the DTIA if necessary, follow guidance from the EDPB
			Consider shortening the retention period of 180 days
			Consider creation of a second Trust & Safety Team in the EU for EU customers
4.	Lack of transparency Account and Diagnostic Data	Study current and future Zoom documentation: inform end-users about the contractual privacy guarantees for the processing	Publish centrally accessible, exhaustive, and comprehensible documentation about the different types of Diagnostic Data, keep the new documentation up to date
		As soon as Zoom makes this possible: show organisation's own privacy conditions for the use of Zoom during sign-up.	
5.	Difficulty to exercise Data Subject Access Requests	Regularly use new access tools when Zoom makes those available: to honour individual requests from employees/students, and as admins, to check compliance with public documentation	Build the agreed improved access-tool for admins to take-out all personal data per end user [by the end of 2022]
			Create a self-service access tool for end users [by the end of 2022]
		Inform employees how they can access their personal data in the available admin log files and reports	Until completion of the self-service tools: provide complete and timely answers to data subject access requests

6.	Employee monitoring system	Create a policy to prevent use of audit logs and reports as an employee monitoring tool	Develop an easier take-out for log files of admin behaviour [by the end of 2022]
		Regular check the logfiles with admin behaviour to verify compliance	

Conclusions

If and when Zoom and the Dutch universities and government organisations apply all the agreed and recommended measures, there are no known high risks for the individual users of the Zoom videoconferencing services.

Caveat. It is uncertain how the transfer risks will be assessed by the national data protection authorities, in their joint investigation into the use of cloud services by public sector organisations. The results are expected by the end of 2022. For this DPIA the transfer risks have been rigorously assessed, including a separate DTIA. Zoom has committed to follow recommendations from the EDPB, and to loyally collaborate with SURF and the Dutch government to update the DTIA when necessary.