



Update DPIA Zoom Education

SURF

Public version

3 April 2024

Privacy Company

Sjoera Nas and Floor Terra,

with help from Jacob Gursky



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
1.4	1 December 2023	Update DPIA, part A review of agreed mitigating measures
1.5	23 January 2024	Input Zoom processed
1.6	12 February 2024	Final version for confidentiality review by Zoom
1.7	13 March 2024	Track changes
1.8	3 April 2024	Public version



Contents

Summary	8
Introduction.....	14
Part A. Description of the data processing	26
1. The processing of personal data.....	26
1.1. Content Data.....	28
1.2. Diagnostic Data.....	29
1.3. Account Data (end users and administrators).....	32
1.4. Account Holder Business Data.....	35
1.5. Support Data.....	35
1.6. Website Data	37
1.7. Feedback and Marketplace Data	38
2. Legal facts: enrolment framework.....	42
2.1. The enrolment framework for Zoom Meetings.....	43
2.2. Differences SURF DPA and global DPA	44
2.3. Agreed action plan mitigating measures	45
2.4. Zoom's change of global terms and conditions in March 2023.....	46
2.5. Definitions of different types of personal data.....	46
3. Technical facts: Diagnostic Data	48
3.1. Audit logs and reports	49
3.2. Telemetry Data	54
3.3. Data Subject Access Requests (DSARs).....	59
3.4. Website Data (cookies and similar technologies).....	71
3.5. Types of personal data and data subjects	75
4. Data processing controls	80
4.1. Privacy controls for end users	80
4.2. Privacy choices and default settings for users when they participate in a meeting.....	87
4.3. Privacy controls for admins	87
5. Purposes of the processing	100
5.1. Purposes education and research organisations.....	101
5.2. Purposes Zoom	101
6. Processor or (joint) controller	110
6.1. Definitions.....	110
6.2. Data processor.....	111
6.3. Subprocessors.....	112
6.4. Data controller.....	118

7. Interests in the data processing	123
7.1. Interests education and research organisations	123
7.2. Interests of Zoom	124
7.3. Joint interests	127
8. Transfer of personal data outside of the EEA	127
8.1. Zoom’s factual transfers of personal data	127
8.2. GDPR rules for transfers of personal data	128
8.3. European Commission Adequacy decision	129
8.4. Standard Contractual Clauses	129
9. Techniques and methods of the data processing	131
9.1. Types of encryption	131
9.2. Aggregation and anonymisation	133
9.3. Privacy by design and privacy by default	134
10. Additional legal obligations: e-Privacy Directive	135
11. Retention periods	138
11.1. Content Data	141
11.2. Diagnostic Data	142
11.3. Account Data	143
11.4. Website Data	144
Part B. Lawfulness of the data processing	145
12. Legal Grounds	145
12.1. Zoom as processor	146
12.2. Zoom as authorised data controller	150
13. Special categories of data	154
14. Purpose limitation	155
15. Necessity and proportionality	156
15.1. The principle of proportionality	156
15.2. Assessment of the proportionality	156
15.3. Assessment of subsidiarity	159
16. Data Subject Rights	159
16.1. Legal framework and contractual arrangements	160
16.2. Right to information	160
16.3. Right to access	160
16.4. Right of rectification and erasure	162
16.5. Rights to object against direct marketing and profiling	163
16.6. Right to data portability	164
16.7. Right to file a complaint	164
Part C. Discussion and Assessment of the Risks	165

17. Risks	165
17.1. Identification of risks	165
17.2. Assessment of Risks	166
17.3. Summary of risks	171
Part D. Description of risk mitigating measures	173
18. Risk mitigating measures	173

Overview of figures and tables

Figure 1: Content Data, Functional Data and Diagnostic Data	26
Figure 2: Registration for a new Zoom account in an Enterprise/Education license	32
Figure 3: Optional information in Zoom account profile	34
Figure 4: New Zoom request for transfer outside of EU office hours	36
Figure 5: Zoom internal support employee training slides	37
Figure 6: Zoom Feedback question	39
Figure 7: Alternative way for end users to provide Feedback to Zoom	40
Figure 8: Zoom App Marketplace	42
Figure 9: Message informing user third party apps are unavailable	42
Figure 10: Zoom Usage Reports	50
Figure 11: Zoom User Activity Reports	53
Figure 12: Screenshot new Telemetry toggle (since 16 December 2023)	55
Figure 13: Example of Telemetry event from Zoom on MacOS	57
Figure 14: Another telemetry example from Zoom on Windows (28 November 2023)	58
Figure 15: Data & Privacy menu available to account owners	62
Figure 16: The list of files returned through the self-service DSAR tool	63
Figure 17: Example of CustomersLoginRecords.txt	65
Figure 18: Tool for account owners to track data subject requests	67
Figure 19: The tool provided to owner accounts for tracking administrator use of DSAR tools	67
Figure 20: DSAR form when Zoom is data controller	68
Figure 21: Zoom instruction to contact the account owner	69
Figure 22: Marketing Preferences menu	70
Figure 23: Zoom Cookie Consent Manager	71
Figure 24: Zoom default cookie settings for EU visitors	72
Figure 25 Cookies on Zoom home page (3 November 2023)	74
Figure 26: Permissions required in the Android Meetings app	81
Figure 27: Permissions required in the iOS Meetings app	81
Figure 28: Request for permissions third party app	83
Figure 29: Menu with main options for hosts	83

Figure 30: Approving or blocking users from specific regions	86
Figure 31: Meeting disabled on web browser when end-to-end encryption is enabled	88
Figure 32: Zoom options to custom available data center regions.....	89
Figure 33: Zoom explanation about account permissions for apps	95
Figure 34: Webinar Registration settings: social share enabled	96
Figure 35: Administrator control for enabling tracking pixels	96
Figure 36: Webinar host enabling a tracking pixel	97
Figure 37: Tracking pixel present on a webinar registration page.....	98
Figure 38: Default settings for the livestreaming of webinars.....	99
Figure 39: Administrator control for third party surveys	99
Figure 40: Owner and Administrator controls for the Zoom AI Companion.....	100
Figure 41: Zoom internal mandatory Privacy by Design questions	109
Figure 42: Zoom blog about compelled disclosure to government authorities	121
Figure 43: First half of 2023: Zoom received 1 subpoena for data from a customer in NL.....	122
Figure 44: Diagram of aggregation provided by Zoom.....	134
Figure 45: Timeline new ePrivacy Regulation	137
Table 1: Overview of recommended measures for organisations	12
Table 2: Tested app versions per operating system	22
Table 3: Zoom list of authorised subprocessors for EU Education customers	113
Table 4: Zoom data retention periods	139
Table 5: Overview of recommended measures for organisations	173

Summary

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

This Update Data Protection Impact Assessment (DPIA) verifies if Zoom has taken all the risk mitigation measures agreed in February 2022. The research was commissioned by SURF, the collaborative organisation for IT in Dutch higher education and research. SURF took the lead in negotiations with Zoom after a first DPIA, from May 2021, showed 9 high data protection risks. This first DPIA was commissioned by the Strategic Vendor Management office for Microsoft, Google Cloud, and Amazon Web Services (SLM Rijk) of the Dutch government, together with the Ministry of the Interior and Kingdom Relations, and SURF.

In February 2022 SURF published a new DPIA, based on the new contract and the new data processing agreement between SURF and Zoom. This DPIA concluded that there were only six low data protection risks provided that Zoom met all the strict deadlines in the agreed action plan to mitigate the high risks. This Update DPIA verifies Zoom's progress with the action plan, and includes the previous DPIA to the extent still relevant.

Scope of DPIA

This Update DPIA is based on a legal analysis of the available (updated) documentation about Zoom Meetings, Chat and Webinar and input from Zoom on the action plan. This Update DPIA does not repeat the full technical inspection of all data processing on the five platforms, as the previous DPIA already concluded that Zoom had taken adequate data processing minimisation measures. This DPIA does not analyse the data processing of Zoom's AI Companion (introduced in September 2023).

For this update report, the inspection was focussed on new tools introduced by Zoom such as the telemetry viewer and the tool for admins to answer data subject access requests, as well as compliance measures regarding cookies.

This DPIA covers the data processing via the paid services offered as Zoom Education, 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 use of the Microsoft Outlook add-in was tested, as well as the usage of cookies and similar technology on the publicly accessible and restricted access Zoom website.

Personal data

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 Education customers)
- Website Data
- Support Data
- Other Data: Feedback and Marketplace

Outcome: no more known data protection risks

Zoom has taken many measures to mitigate the remaining low risks. If schools and universities follow the recommendations in [Table 1](#) below, all known data protection risks are mitigated.

- Zoom is a US based company. To alleviate concerns from EU-customers about **transfers of personal data to the USA**, Zoom already offered end-to-end-encryption for all Content Data exchanged in Zoom meetings and webinars since November 2020. This ensured that Zoom was unable to provide access to the streaming Content Data in clear text/audio/video if compelled by government authorities. Additionally, Zoom committed to offer EU-only processing for all personal data (Content, Account, Diagnostic, Support and the restricted access Website Data) for its EU Education customers, by the end of 2022. Zoom has effectively realised this EU-cloud in a number of phases. Since mid-2022, Zoom offers European organisations the possibility to have all of their Support Data exclusively processed in the EU. If they wish support outside of regular working hours in the EU, they can give specific case-by-case consent to the transfer of the personal data to a helpdesk outside of the EU (in the USA or the Philippines). The only ongoing systematic transfer of data outside of the EU after the end of 2022 is the transfer of pseudonymised user account data to the USA to allow users to log into their account. Once the user is identified, personal data are exclusively processed in the EU. Additionally, Zoom transfers aggregated non-personal Diagnostic Data to Zoom in the USA. Incidentally, some personal data may be transferred to the Trust & Safety team in the USA, for example in case of a complaint, or transferred to a third country in case Zoom were to receive an order for compelled disclosure from a government authority. Contractually all transfers are based on the EU Standard Contractual

Clauses (SCCs Controller to Processor). Because Zoom has registered itself as participant to the EU US Data Privacy Framework no supplemental measures are required anymore to protect special categories of data. Zoom does not systematically transfer personal data from its EU Education customers to third countries. Though Zoom includes subprocessors in third countries in its public subprocessor list, these transfers only take place if EU end users make conference calls while they are physically outside of the EU.

- Based on the new DPA with SURF from February 2022, **Zoom is a data processor for all personal data**, except when authorised to ‘further’ process some personal data as an independent controller, and in relation to its publicly accessible website. The DPA includes a limitative list of purposes for which Zoom is authorised to ‘further’ process some personal data as an independent data controller, when strictly necessary for its own legitimate business purposes. 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. These guarantees also apply to guest users that join a meeting organised by an EU Education customer. Zoom’s data processing agreement with SURF is different from Zoom’s global data processing agreement. Zoom has updated its global DPA to include many of the negotiated improvements, but will also publish an addendum for EU/EEA Education customers in the first half of 2024.
- Zoom uses third parties for some data processing. Zoom has asserted 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.

Zoom has published its data retention schedule on 29 March 2024. In the dialogue with SURF, Zoom has **clarified and minimised the data retention periods**, to an average of 7 to 31 days for most of the Content and Support Data after account termination, and 12 to 15 months after creation of the Diagnostic Data (with the exception of security logs). These retention periods start with the adoption of the new DPA by each customer. Zoom has created a new possibility for admins to individually delete personal data. Zoom retains IP addresses from all end users for 10 years, to comply with US fiscal law, but reduces identifiability by clipping the last octet from IPv4 addresses and the last 64 bits of IPv6 addresses before storing these identifiers in a separate container.

- Zoom has become **more transparent about the Diagnostic Data** it processes. Zoom had published a list of telemetry events it collects, but published an updated Cookie Policy on 23

June 2023¹ and expanded the information in its Data Privacy Data Sheet with information about all metadata, data transfers and subprocessors in April 2023.² The support page with the detailed information about the Telemetry Data was offline at the end of 2023, but a new version was published on 1 March 2024.³ Zoom has also implemented a telemetry toggle for admins to opt-in to the collection of additional telemetry. Zoom has confirmed in the EU it only collects required telemetry as the default option.

- Zoom has developed self-service tools for administrators to file Data Subject Requests , as well as a take-out tool for logs of admin behaviour, Zoom has also improved the understandability of the output of the DSAR results by providing descriptions of each file.⁴
- 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 Education account end users for consent for new features. Only the admin is able to enable new data processing, with an active opt-in. This new processing includes Zoom’s AI Companion, which must be enabled by an administrator and offers only a portion of its larger set of features. This policy also applies to new AI functionalities: they are disabled by default.
- Like all other US 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.
- 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 has developed a marketing preferences self-service tool that end users can use to opt-in to marketing lists, and sales contacts can use to opt-out.
- Zoom has agreed to take two additional measures by the end of 2024 the latest. Zoom will release a Diagnostic Data Viewer for the Telemetry Data in the first half of 2024 and build tools for Education end users for direct access to data & privacy tools in the second half of 2024.

¹ Zoom, Cookie Statement, last updated 30 June 2023, URL: <https://explore.zoom.us/en/cookie-policy/>.

² Zoom, Privacy Data Sheet, last updated April 2023, URL: <https://explore.zoom.us/media/privacy-data-sheet.pdf>.

³ Zoom Meeting, Webinar, and Team Chat Telemetry Events, last updated 1 March 2024, URL: https://support.zoom.com/hc/en/article?id=zm_kb&sysparm_article=KB0074458.

⁴ Zoom, Using Data & Privacy for data management, last updated 27 February 2024, URL: https://support.zoom.com/hc/en/article?id=zm_kb&sysparm_article=KB0057736.

Table 1: Overview of recommended measures for organisations

Low risks	Measures gov orgs and universities
Loss of control, loss of confidentiality due to unauthorised access to Content Data	<p><u>Consider</u> enforcing the use of E2EE as a good security measure. This is no longer required to mitigate data transfer risks.</p>
	<p>Consider use of the available privacy options such as:</p> <ul style="list-style-type: none"> • 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 • Enable the waiting room for participants
	<p>Create policy rules to prohibit the use of confidential data in room and topic names. If necessary for internal confidentiality requirements: draft a policy to instruct users if they can or must use a profile pictures.</p>
	<p>Conduct a Fundamental Rights Algorithm Impact Assessment (FRAIA) prior to enabling new features of Zoom’s AI Companion.</p>
Loss of control, loss of confidentiality due to incidental transfer of personal data to third countries	<p>Organisations are advised to carefully assess optional third party integrations offered by Zoom, not enable Giphy, and use their own GDPR-compliant subprocessors to send invitations for Zoom webinars. If the organisation uses Zoom’s subprocessor Twilio to send webinar invitations: do not enable the tracking pixel, or ask for prior unambiguous consent for this tracking from the recipients, provided that the recipients are legally able to freely give such consent (difficult for employees).</p>
	<p>Enable (or do not disable) ‘EU-only’ for Support requests. Draft an instruction for admins when they can consent to export of Support Data to the USA and the Philippines in exceptional emergency circumstances outside of EU office hours.</p>
	<p>Use Single Sign On to further reduce the transfer risks of pseudonymised e-mail addresses to Zoom in the USA (necessary when logging-in).</p>

Lack of transparency Account and Diagnostic Data	Use the Vanity URL like universityofamsterdam.zoom.us in combination with Single Sign On (SSO) to be able to show the organisation’s own privacy policy and use conditions during sign-up, and on all meeting, webinar, and recording registration pages. Alternatively, if the organisation does not use SSO and end users must individually sign-up: tell them Zoom’s general consumer privacy policy and TOS do not apply.
Difficulty to exercise Data Subject Access Requests	Zoom has developed a self-service tool for admins. Inform parents, students and employees how they can file a data subject access request with the school or university administrator. By the end of 2024, end users should be able to file a DSAR directly, via a new DIY portal. Zoom will also release a Diagnostic Data Viewer for the Telemetry Data before June 2024.
Employee monitoring system	Create a policy to prevent abuse of audit logs and reports as an employee and admin monitoring tool
	Regularly check the logfiles with admin behaviour to verify compliance

Conclusions

Zoom has taken most of the agreed measures to mitigate the remaining low data protection risks, and will take the two remaining agreed measures by the end of 2024 at the latest.

Zoom now processes most of the personal data from Dutch Education customers exclusively in the EU. Zoom does not systematically transfer personal data to third countries outside of the EU, only incidentally, if an end user travels outside of the EU, if an admin consents to a one-off transfer to get support outside of office hours, in case of a complaint or security flag, or in case Zoom sends a service notification through its subprocessor Twilio from the USA.

Zoom does systematically transfer pseudonymised account data and IP addresses to the USA, but because of the new EU adequacy decision for the USA in July 2023, and because Zoom is a participant to the EU US Data Privacy Framework, there are no more high risks resulting from these data transfers to the USA. **If the Dutch education and research organisations apply the recommended measures, there are no known data protection risks for the individual users of the Zoom videoconferencing services.**

Introduction

This DPIA was originally commissioned by SURF (the collaborative organisation for IT in Dutch higher education and research the organisation) and two Dutch ministries. After an initial version was provided to Zoom, SURF took the lead in the negotiations with Zoom and commissioned an updated report with the outcomes of the negotiations with Zoom. SURF published the DPIA on 22 February 2022.⁵ This DPIA reflected commitments by Zoom to implement technical measures to mitigate data protection risks. This Update DPIA contains the verification if Zoom has taken the agreed measures, and if these measures have mitigated the remaining low data protection risks.

Scope

This DPIA examines the data processing via Zoom's paid services offered to EU customers with Education licenses. The conclusions from this DPIA also apply to Zoom's EU 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."*⁶

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.

⁵ SURF, DPIA Zoom Education and Enterprise, Public version 1.3, 25 February 2022, URL: https://www.surf.nl/files/2022-03/dpia-zoom-25-february-2022_0.pdf.

⁶ Zoom Services Description, 19 January 2024, URL: <https://zoom.us/docs/en-us/services-description.html>.

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 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.⁷

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 education and research 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.⁸

If Dutch organisations would use Zoom Education services, this would involve processing of data from and about the communication (content and metadata). Because Zoom Education 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

⁷ *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>.

⁸ 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>.

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 administrators) lead to a systematic observation of the behaviour of employees, especially in view of the increased use of videoconferencing tools for day-to-day work (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 Education services are in an unequal relationship of power with the education and research organisations. This also includes job applicants.⁹
- 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.”¹⁰

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.”¹¹

Criteria Dutch Data Protection Authority

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

“Communications data (criterion 13). Large-scale processing and/or systematic monitoring of communications data including metadata identifiable to natural persons, unless and as far as this is

⁹ 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.

¹⁰ 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.

¹¹ Idem, p. 14.

necessary to protect the integrity and security of the network and the service of the provider involved or the end user's terminal equipment.”¹²

This criterion may apply to Zoom’s Education services, as the monitoring of communications 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, organisations must first conduct a DPIA (or have it performed). This DPIA examines the necessity for Zoom to collect and store the communications data, as well as the necessity and circumstances in which the employer can use these communications data.

In GDPR terms, SURF is **not the data controller** for the processing of personal data via the use of the Zoom Education services. However, as central negotiator for many cloud services, SURF has commissioned this DPIA in acceptance of its legal responsibility to assess the data protection risks for employees and students, and to negotiate for a framework contract. Therefore, this umbrella DPIA is meant to assist education and research institutions 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 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.

Hence, this umbrella DPIA cannot replace the specific risk assessments the individual 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.¹³ 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*, but in an Enterprise tenant. However, Zoom explained that in principle, the Education versions were identical in data processing at the time of this investigation¹⁴, 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 Education is that Zoom Education offers advanced administration controls and the capacity to organise Webinars.

¹² Dutch DPA, (in Dutch only), list of DPIA criteria published in the Staatscourant (Dutch Government Gazette) of 27 November 2019.

¹³ Zoom, Choose a plan, URL: <https://zoom.us/pricing>.

¹⁴ 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.

Scope of this DPIA: Zoom Education and Zoom Education

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
- 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 any Zoom product other than Meetings and Chat, such as:

- Zoom Phone
- Zoom Rooms for Conference Rooms¹⁵
- Zoom Video Webinars¹⁶
- 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.
- Zoom AI Companion: introduced in September 2023.¹⁷

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 Education.

Legal fact-finding

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

¹⁵ 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.

¹⁶ Zoom's 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.

¹⁷ Zoom blog, Meet Zoom AI Companion, 5 September 2023, URL: <https://blog.zoom.us/zoom-ai-companion/>. See also Zoom, Zo haal je alles uit Zoom AI Companion: gids om aan de slag te gaan met je AI-assistant, 26 januari 2024, URL: <https://www.zoom.com/nl/blog/zoom-ai-companion-getting-started-guide/>

20 November 2020. On behalf of Privacy Company, a letter was sent 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, Privacy Company held two conference calls with Zoom on 4 and 11 December 2020.

In March 2021, Zoom replied to the factual findings. In May 2021, the first DPIA was completed and shared with Zoom. SURF, Zoom and Privacy Company have since engaged in a structural dialogue. In February 2022 a new version of the DPIA was published based on the new framework contract and improved data processing agreement. The framework included an action plan with strict deadlines for Zoom to implement mitigating measures. Between March 2022 and March 2024 (completion of this Update DPIA), SURF, Zoom and Privacy Company had many meetings and e-mail exchanges with Zoom to check the progress with the action plan, but also to discuss new features and developments with regard to the use of AI and for example the methodology of aggregation.

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 the DPIA from February 2022 (*Technical analysis Zoom Education*), 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 university. The scenarios were executed on 30 September 2020 (iOS, macOS, Windows and Android apps).

Privacy Company exported 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](#).

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, Privacy Company filed two formal GDPR Data Subject Access Requests (DSARs) with Zoom on 12 October 2020, 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 initially tested the software on the different platforms with the then most up to date versions, plug-in, and Chrome browser.

In the period between May 2021 and March 2024 Privacy Company repeatedly checked the admin console and publicly available documentation, but did not perform a complete retest. Prior to the finalisation of this Update DPIA, Privacy Company did perform a retest with the new tools for admins

to honour data subjects requests, exported admin logs and intercepted the Telemetry Data from the Zoom application on a Windows 10 Pro machine version 22H2. Tests of the browser based accounts settings were performed on the same Windows machine with an up to date Firefox web browser.

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.

Table 2: Tested app versions per operating system

Operating system	Zoom client or app first test run September 2020	Zoom app second test run November 2020	Zoom retests November 2023
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 (<i>Click and Run</i>) App version 5.3.52819.0925		
Windows 10 Pro 19045.3693			Firefox version 120.0 (64-bit) (<i>Click and Run</i>) App 5.16.6 (24712)

Summary of mitigating measures Zoom since February 2022

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 Education customers factually qualified as joint controllers, and did not have a legal ground for the data processing.

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 signed a new contract, a Data Processing Agreement (DPA) and an action plan with firm deadlines to mitigate all of the high risks. Zoom agreed to apply most of these improvements to all of its EU Education customers. Zoom had already modified its public DPA to reflect many of the improvements, but Zoom agreed to also make a specific EU/EEA DPA addendum available for SURF customers. Because Zoom agreed to become a data processor for all personal data (except for its public Website Data), and to only process the personal data for a limitative list of necessary purposes, many high risks were already mitigated in February 2022. However, the mitigation of some risks required the implementation of new technical measures. These could not immediately be realised, but Zoom did commit to a set of agreed deadlines for implementation.

Since the winter of 2021, Zoom has taken the following mitigating measures:

- Created an offer to exclusively process most of the personal data from EU Education customers in the EU by the end of 2022. Since mid-2022, Zoom offers European organisations the possibility to have all of their Support Data exclusively processed in the EU. If they seek support outside of EU office hours they can provide specific consent for the incidental transfer of personal data outside of the EU through a new pop-up request.
- Published an updated Data Privacy Sheet (April 2023).
- Added categories of personal data to the Privacy Data Sheet that were omitted initially.
- Chosen a method to aggregate diagnostic data in the EU before transfer to the USA for further processing for legitimate business purposes such as account and usage statistics.
- Applied privacy by default settings (no tracking cookies) to the restricted access web pages (Portal and sign-up), applied a correct cookie consent banner to the public website (November 2021) and disabled the tracking pixel in functional e-mails to users (sent through subprocessor Twilio).
- Provided a public explanation for admins about the use of a vanity subdomain and use of Single Sign On.
- Created an improved access-tool for admins to take-out all personal data per end user.
- Created an admin interface to easily grant requests from data subjects for access to, or deletion of their data.
- Stopped collecting the unencrypted Passcode in the audit log files.
- Created an option to view logs with actions of administrators, including records of requests related to data subject rights.
- Improved the understandability of the DSAR output by grouping the results per used service.

- Expanded the help article for admins with detailed information about the results of DSARs.

Zoom has committed to realise three other privacy improvements in the near future:

- Publication of retention periods of the different personal data (29 March 2024)
- Releasing a Diagnostic Data Viewer for end users to see what Telemetry Data Zoom collects from their device (anticipated in the first half of 2024)
- Building a tool for Education end users to access data & privacy tools (second half of 2024)

Outline

This assessment follows the structure of the *Model Gegevensbeschermingseffectbeoordeling Rijksdienst (PIA)* (September 2023)¹⁸, with some modifications. 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.

¹⁸ The Model Data Protection Impact Assessment federal Dutch government (PIA) version 3.0. see: <https://www.kcbr.nl/sites/default/files/2023-09/Model%20DPIA%20Rijksdienst%20v3.0.pdf>.



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 be taken by Zoom and the individual education and research organisations to mitigate the remaining low risks identified in this DPIA, as well as their impact.

This DPIA was conducted between September 2020 and March 2024.

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 Education Meetings.

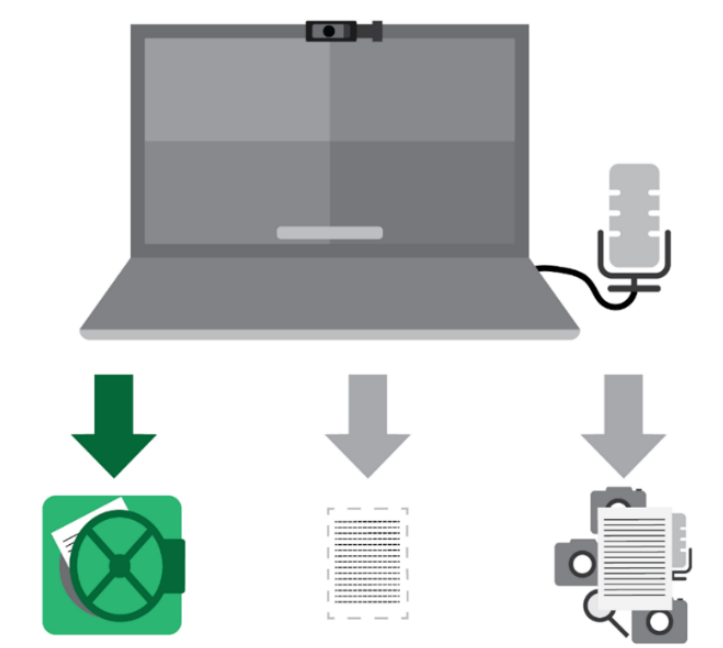
This Part A starts with a short description of the processing of different kinds of data. It continues with a description of the different categories of personal data that may be processed in the Diagnostic Data, the categories of data subjects that may be affected by the processing, the available privacy 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 education and research 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



Broadly speaking, the use of Zoom's cloud services involves three main categories of data:

Content Data are the data exchanged in real-time meeting and webinar video, audio, and shared content during the hosting of meetings and webinars including chats and 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 Webinar functionalities, including all possible features, as well as use of the (free and paid) Zoom account. Diagnostic Data include **Website Data** (including cookies) and **Telemetry Data**. **Telemetry Data** are personal data collected in the applications on the end user device about the use of the service, and regularly sent to Zoom via the Internet.

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.

Additionally, four more categories of personal data can be identified:

Account Data from **end users** and **admins**. These data can be part of both Content and Diagnostic Data.

Account Holder Data from sales contacts from Zoom such as procurement officers.

Support Data include both the specific content of a support request filed by an admin, as well as Zoom's administration of support contacts and recommended measures.

Feedback Data when end users provide information to Zoom about the functioning of the service

In its updated (April 2023) Privacy Data Sheet, Zoom defines 6 categories of personal data: Customer Content, Diagnostic Data, Account Data (end users), Account Holder Data, Support Data, Website, and Feedback Data. For each category, Zoom describes the detailed contents.¹⁹

¹⁹ Zoom, Privacy Data Sheet, last updated April 2023, URL: <https://explore.zoom.us/media/privacy-data-sheet.pdf>.

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 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). Since the end of 2022 this choice also means the Diagnostic, Support, and Account Data of end users are exclusively processed in the EU, including the contacts and calendars they actively import in their Zoom services. The remaining incidental transfers of personal data to the USA and other 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 (* is not possible if E2EE is enabled)
 - Video, audio, whiteboard, captions, and presentations
 - In-meeting Questions & Answers, polls, and survey information*
 - Closed captioning (Live Transcription)*
 - Chat Messages in 1:1 in-meetings and group chat messages that are not transferred to a permanent chat channel.
 - Customer Initiated cloud recordings*
 - Cloud recording of video, audio, whiteboard, captions, and presentations*
 - Text file of all in meeting group chats*
 - Audio transcript text file*
- Meeting and Webinar Participant Information includes²⁰:
 - 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)

²⁰ The information also included 'user categorisation labels' that organisations could apply to participants. The possibility to create labels has been removed by the end of 2023, but organisations that have used such labels before, can still see the labels in the historical logs.

- Room Names (if used)
- 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 365.²¹
- Calendar Information. This includes meeting schedules made available through Customer controlled integrations (e.g., Outlook, Google).

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 and similar technology 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).

²¹ Idem.

In its Privacy Data Sheet²², 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
 - Performance, troubleshooting, and diagnostics information
- 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).

Zoom explains that Telemetry Data should not include Customer Content, or information about other users, meeting names, or other user-supplied values such as profile names.

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,

²² Zoom, Privacy Data Sheet, last updated April 2023, URL: <https://explore.zoom.us/media/privacy-data-sheet.pdf>.

and some pseudonymous identifiers, including a UUID, userID and meeting_id. Some fields are common for all events:

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

Zoom describes 19 specific required Telemetry events in its public help article in relation the Meeting, Webinar and Chat services in scope of this DPIA²³, and has committed to keep this list 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, but Zoom has since moved some of these events to the category of Optional Telemetry events (727 events in total).

- 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 service notifications, such as “Forgot My Password”, “User has joined your meeting”, and DSAR 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. Zoom also processes the hashed e-mail address plus unique user identifier to allow users to log into their account, and separately retains a record of clipped IP addresses of EU Education users to comply with specific USA tax legislation. These data are only accessible by Zoom employees with a need to know and subject to appropriate technical and organisational measures.

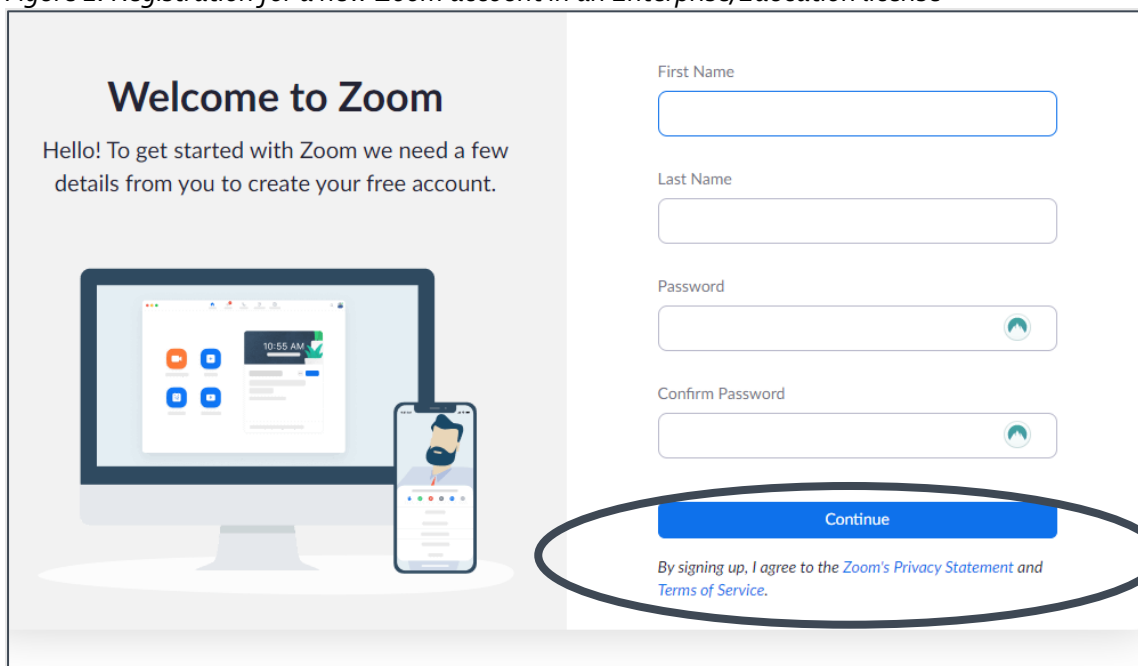
²³ Zoom, Zoom Meeting, Webinar, and Team Chat Telemetry Events, last updated 1 March 2024, URL: https://support.zoom.com/hc/nl/article?id=zm_kb&sysparm_article=KB0074458

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.”*²⁴

Figure 2: Registration for a new Zoom account in an Enterprise/Education license²⁵



Welcome to Zoom

Hello! To get started with Zoom we need a few details from you to create your free account.

First Name

Last Name

Password

Confirm Password

Continue

[By signing up, I agree to the Zoom's Privacy Statement and Terms of Service.](#)

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 Education license may decide through admin settings to only allow participants

²⁴ 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>.

²⁵ Screenshot made on 16 February 2022.

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.²⁶

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 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 Education customers.²⁷

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)."*²⁸

The use of such a tokenised email address helps prevent future data transfer risks. See Section 7 of this DPIA.

End users can choose to actively provide profile data to Zoom, such as a picture, Department, Job Title and Location.²⁹ For this test, a picture was chosen with the words 'top secret' (See [Figure 3](#) below).

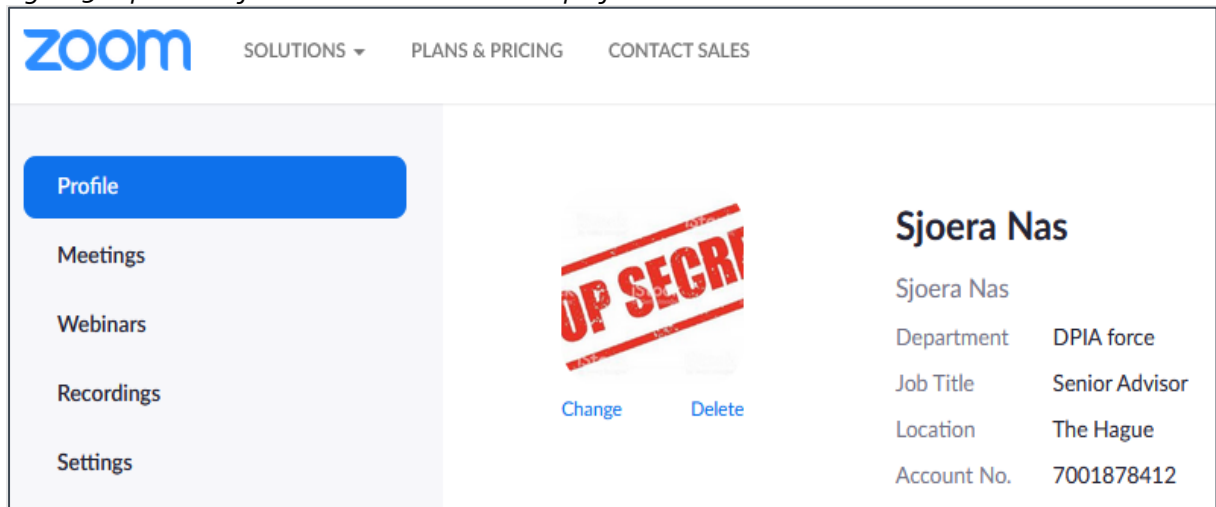
²⁶ Zoom, Authentication Profiles for meetings and webinars, URL: <https://support.zoom.us/hc/en-us/articles/360037117472>.

²⁷ Zoom e-mail to SURF, 14 February 2022.

²⁸ 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>.

²⁹ Users can provide this information through the Zoom Account end user interface, URL: <https://eu01web.zoom.us/profile>.

Figure 3: Optional information in Zoom account profile³⁰



According to Zoom’s Privacy Data Sheet³¹, depending on how the account administrator has configured the Zoom Education 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)
- Additionally, Zoom collects the Zoom unique ID from guest users that connect to a meeting organised by an EU Education customer.

Until the summer of 2021, Zoom also asked for the date of birth when end users signed up for an Education 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 Education customers.

³⁰ Name of researcher intentionally included.

³¹ Zoom, Privacy Data Sheet, last updated April 2023, URL: <https://explore.zoom.us/media/privacy-data-sheet.pdf>.



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 account. Zoom can send 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 Education customers by providing online resources, including a chatbot, and with chat and phone support through the Zoom Support Center.³² Owners and administrators of Education accounts can file online support requests. The request can include attachments, such as screenshots. Such screenshots may include Content Data.

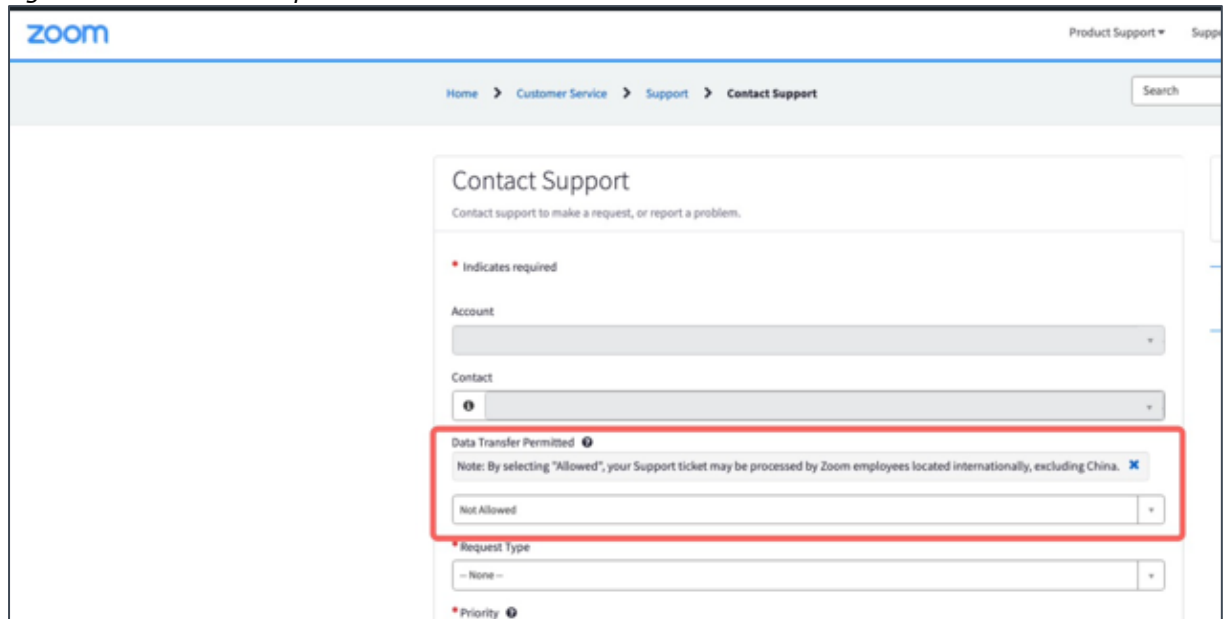
Zoom initially used a USA based subprocessor to provide its Support Services platform, but has replaced this by the German-based subprocessor ServiceNow.³³ Since mid-2022 Zoom exclusively processes Support Data from its EU Education customers in the EU, during EU business hours. The EU support desk works with an EU instance of the ServiceNow platform. For new customers support is provided exclusively by the EU support desk by default, existing EU based customers have to opt-in (to prevent overload).

As shown in [Figure 4](#) below, Zoom has added a specific consent request for admins to agree to transfer of support ticket data outside of the EU when they need 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 admin explicitly consents to such an incidental transfer of Support Data.

³² Zoom technical support, URL: <https://support.zoom.us/hc/en-us/articles/201362003>.

³³ Zoom, Third-Party Subprocessors, effective 3 November 2023, URL: <https://explore.zoom.us/nl/subprocessors/>.

Figure 4: New Zoom request for transfer outside of EU office hours



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

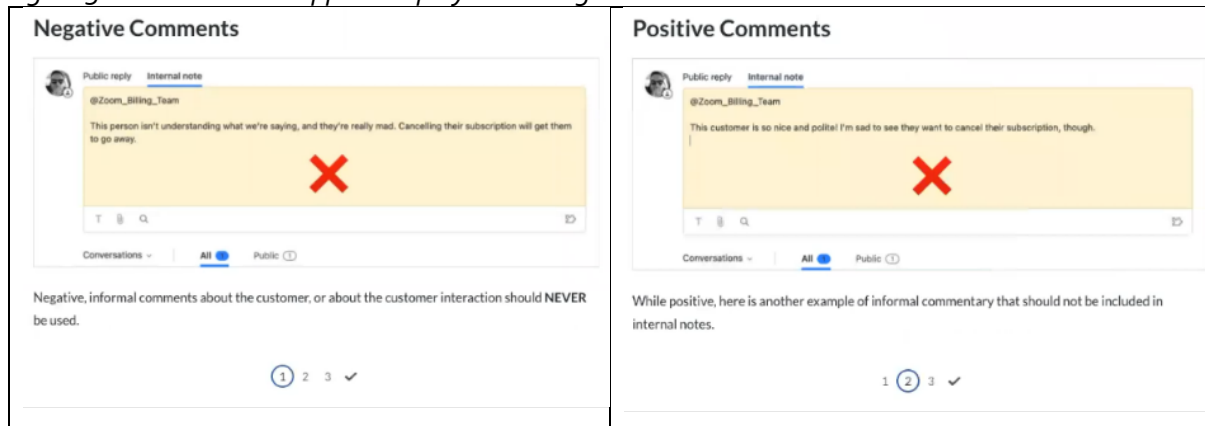
“Support Data is information a customer provides to Zoom or is otherwise processed in connection with support activities such as support bot messages, chats, and phone calls (including recordings of those calls) and Service support tickets. The business contacts for a Zoom Education and Enterprise account 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.”³⁴

Zoom also explains the customer is the controller for the Support Data: *“As controller, Zoom Customers instruct Zoom to process Support Data to provide the requested support, which includes applying knowledge gained from individual customer support requests to benefit all Zoom customers but only to the extent such knowledge is anonymized.”³⁵*

³⁴ Zoom, Privacy Data Sheet, last updated April 2023, URL: <https://explore.zoom.us/media/privacy-data-sheet.pdf>.

³⁵ Idem.

Figure 5: Zoom internal support employee training slides³⁶



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. 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 to a meeting organised by a customer with an EU Education license are automatically redirected to the EU-hosted Zoom pages when they log in, or when they click on a link to join a meeting.³⁷

Zoom is a data controller for its publicly accessible website zoom.us. Both for the restricted and the public website, Zoom commits to only set and read strictly necessary cookies by default for visitors from the EU. Zoom has a separate (updated) Cookie Policy³⁸ and has implemented a cookie consent banner (See [Section 3.5](#) below).

³⁶ Slide deck provided by Zoom on 1 February 2022.

³⁷ As last checked on 27 November 2023, visitors are redirected to the URL: <https://eu01web.zoom.us>.

³⁸ Zoom, Cookie Statement, last updated 30 June 2023, URL: <https://explore.zoom.us/en/cookie-policy/>.

As explained in Section 1.3 customers with an EU Education license can use SSO in combination with a vanity URL, 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 place marketing cookies on such Vanity URLs."*³⁹ 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 describes in its Privacy Data Sheet that its Website Data include:

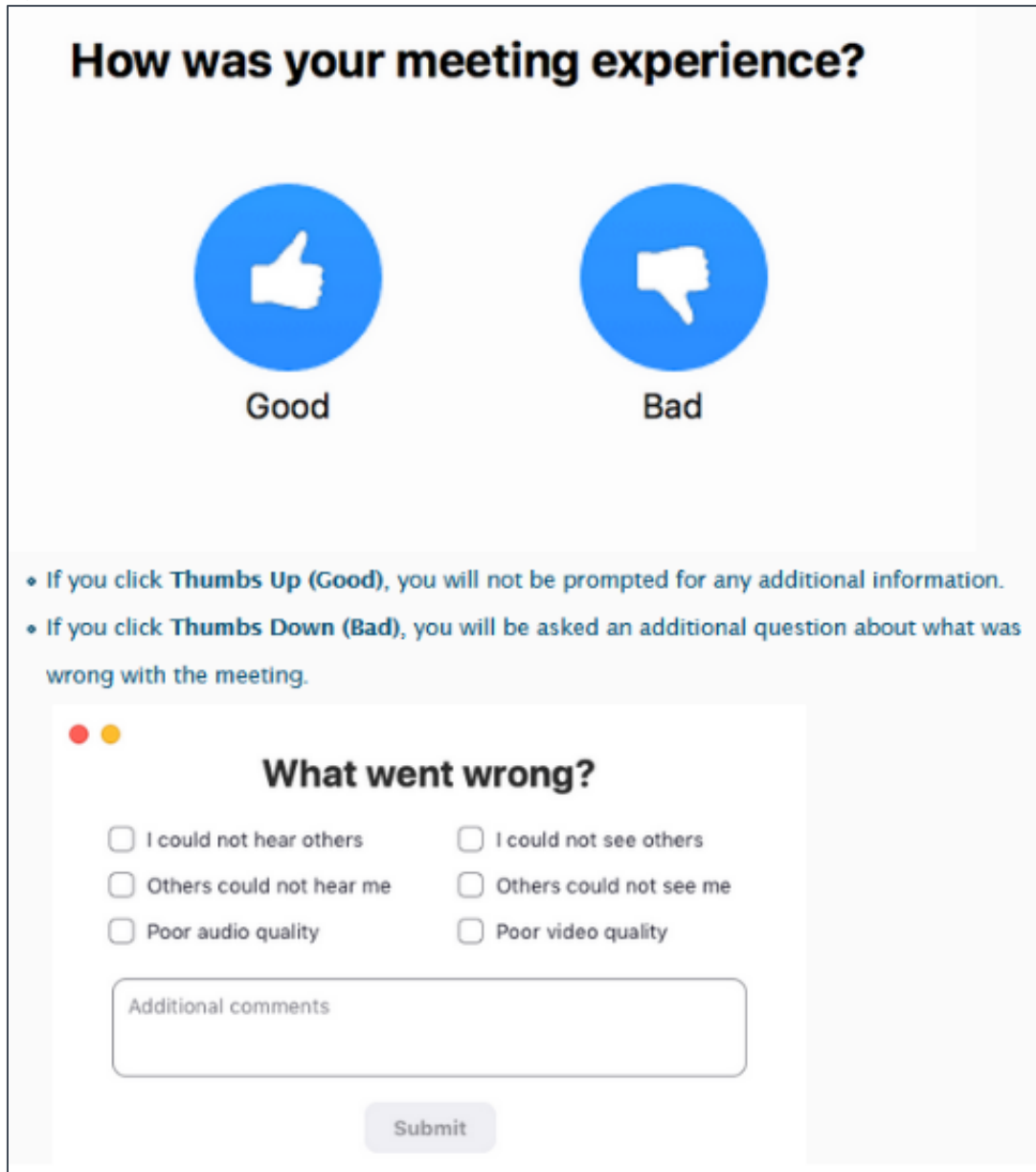
- Strictly necessary cookies as specified in the Cookie Statement
- Internet protocol (IP) address
- Browser type
- Internet service provider (ISP)
- Referrer URL
- Exit pages, the files viewed on our website (e.g., HTML pages, graphics, etc.),
- Operating system
- Date/time stamp
- Approximate location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

³⁹ Zoom reply to part A of the DPIA, 19 March 2021, p. 16.

Figure 6: Zoom Feedback question



How was your meeting experience?

Good **Bad**

- If you click **Thumbs Up (Good)**, you will not be prompted for any additional information.
- If you click **Thumbs Down (Bad)**, you will be asked an additional question about what was wrong with the meeting.

What went wrong?

I could not hear others I could not see others

Others could not hear me Others could not see me

Poor audio quality Poor video quality

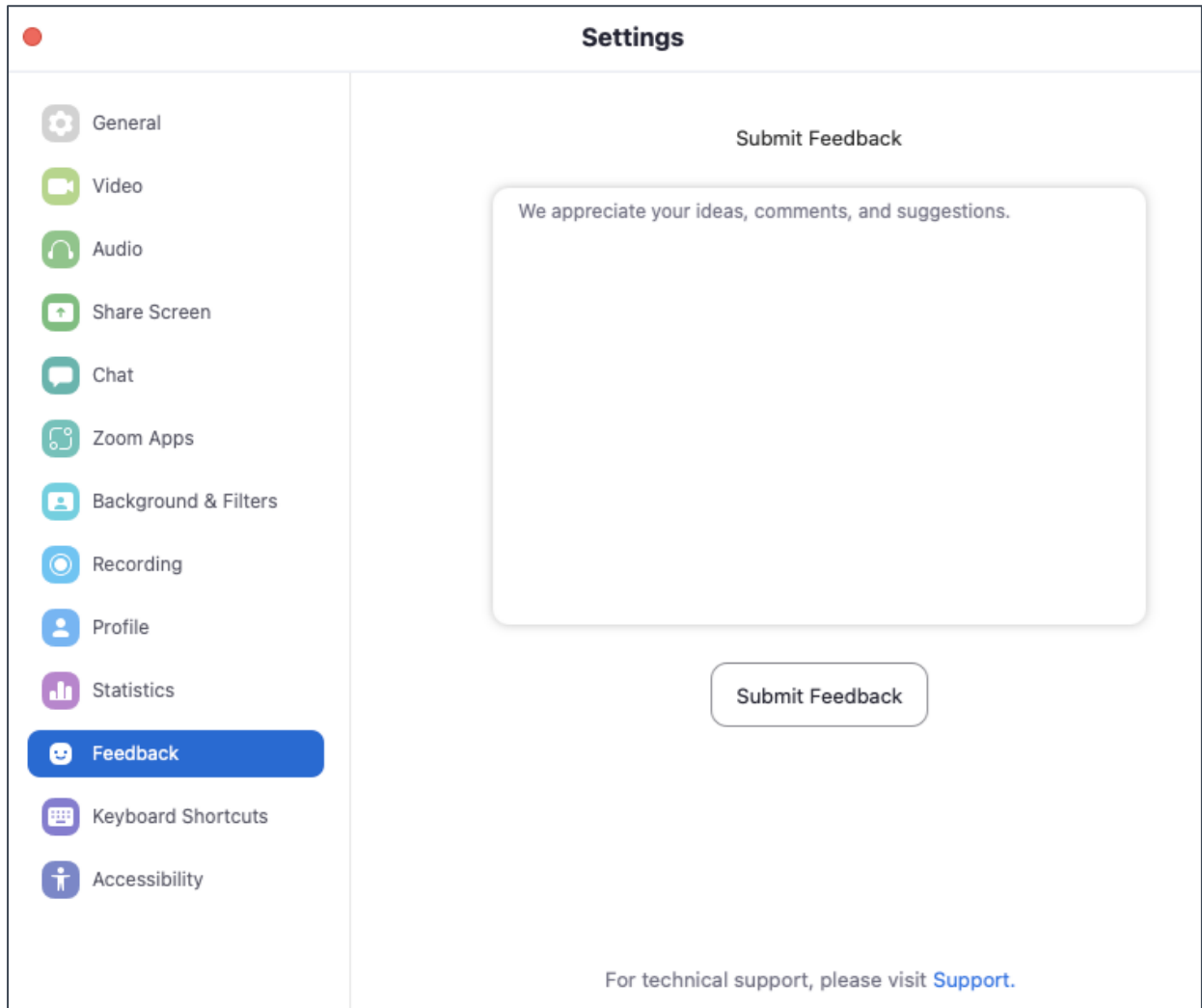
Additional comments

Submit

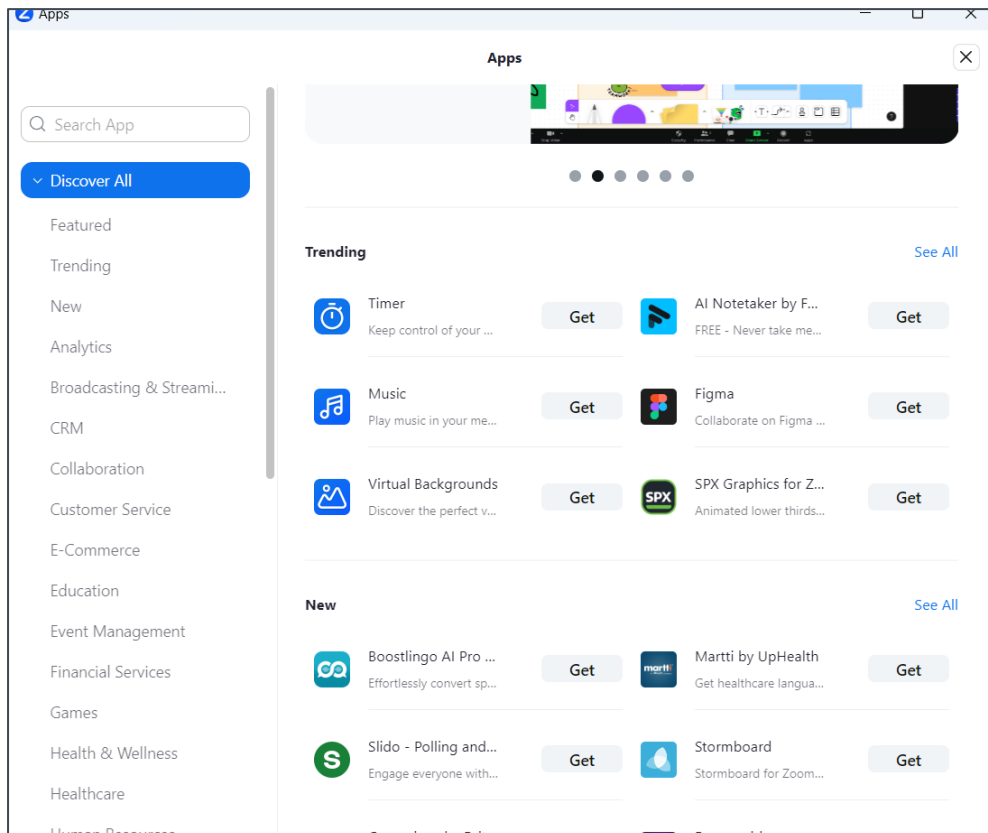
Feedback is a tool that asks end-users to rate the quality of a conference call at the end of a meeting, by selecting a thumbs up or thumbs down icon. If they are not satisfied, they can answer more questions, and enter free text in an open text field. See [Figure 6](#) above.

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. This option 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.

In the DPA with SURF 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. Organisations are advised to develop and implement a policy what apps are permitted, after they have performed a separate DPIA if necessary.

When an owner or administrator enables end to end encryption, as described in Section 4.3.1, third party apps are disabled.

[Figure 9](#) below contains the message shown to a user when the user attempts to select third party apps in a Zoom call that is using end to end encryption.

Figure 8: Zoom App Marketplace

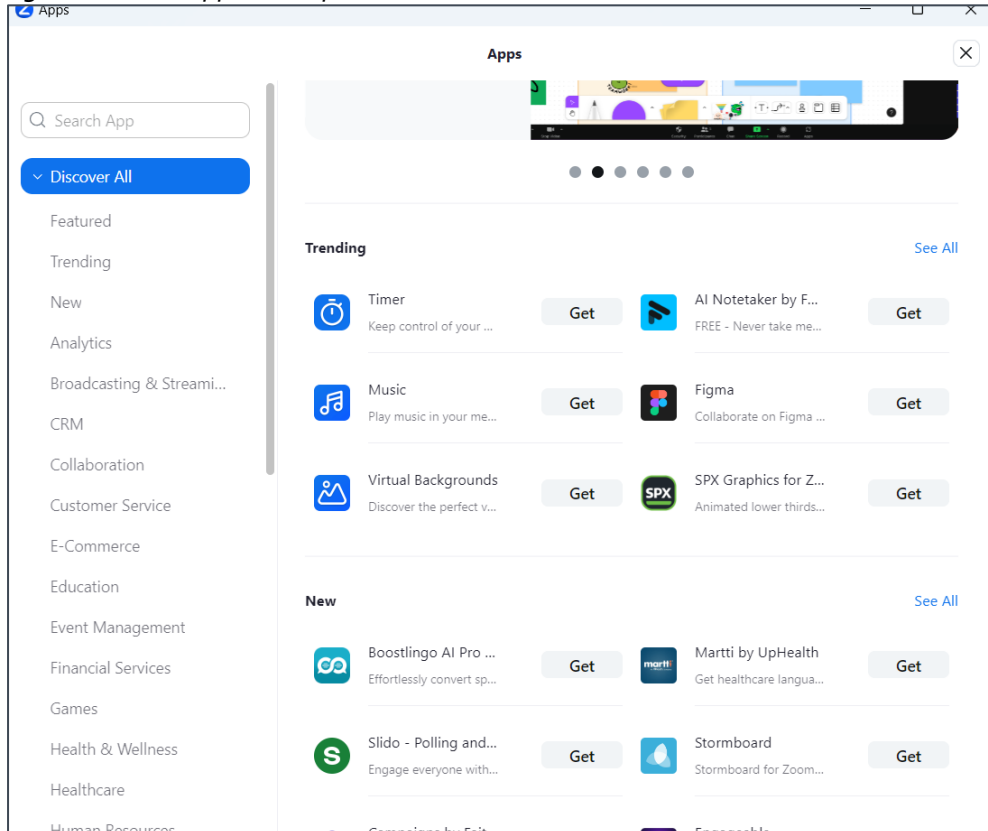
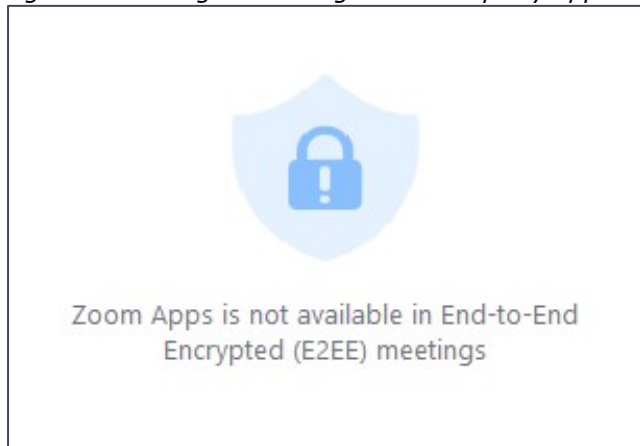


Figure 9: Message informing user third party apps are unavailable



2. Legal facts: enrolment framework

The Dutch government DPIA model prescribes 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 model DPIA, this question is addressed in two separate sections. This Section 2 provides a description of the legal facts and definitions following from the framework contract with Zoom for the Dutch education and research organisations.

Section 3 below 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 latter 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 categories are outlined in Sections 3.5.1 and 3.5.2 of this report.

2.1. The enrolment framework for Zoom Meetings

Zoom's Education services are generally procured online, through the Zoom website. However, SURF works with its own 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 own 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 MSA⁴⁰) (*not for SURF/HEAnet)
- Zoom Services Description (Exhibit A of the customised Zoom MSA)⁴¹ (*not for SURF/HEAnet)
- Zoom (new) Data Processing Agreement (The Addendum or Zoom DPA⁴²) with SURF with appendices

⁴⁰ 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.

⁴¹ Zoom Services Description, effective 19 January 2024, URL: <https://zoom.us/docs/en-us/services-description.html>. A previous version of the content is attached as Exhibit A Services Description to the Zoom customized MSA, dated 8 December 2020.

⁴² SURF has a specific DPA focussed on GDPR obligations. The SURF DPA is comparable but not identical to the Zoom Global Data Processing Addendum, version of March 2023, URL: https://zoom.us/docs/doc/Zoom_GLOBAL_DPA.pdf.

- New (June 2021) Standard Contractual Clauses for the transfer of data from the EU to the USA, Model 1 and Model 2⁴³
- Acceptable Use Policy (Community Standards)⁴⁴ and
- Zoom Cookie Statement.⁴⁵

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 still asks users to accept the applicability of its Privacy Statement and Terms of Service when they create a new Zoom account within the Education license. As explained in Section 1.3, 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 core of the negotiated new enrolment framework is the improved and expanded (new) Zoom DPA for EU Education customers. 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."*⁴⁶ This hierarchy means that nor Zoom nor individual 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. Differences SURF DPA and global DPA

The DPA agreed between Zoom and SURF is distinct from Zoom's global DPA. Though the dialogue with Zoom has resulted in many systemic changes for all global customers, and hence, to a completely overhauled global DPA, there are still some differences between the SURF DPA and the global DPA. Zoom applies the SURF DPA to all its EU and EEA Education customers, and has committed to publish

⁴³ 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.

⁴⁴ Zoom Community Standards, undated, URL: <https://zoom.us/docs/en-us/community-standards.html>.

⁴⁵ Zoom, Cookie Statement, last updated 30 June 2023, URL: <https://explore.zoom.us/en/cookie-policy/>.

⁴⁶ 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."*

a specific addendum for EU Education customers in the first half of 2024. In this DPIA, whenever the abbreviation DPA is used, it refers to the DPA negotiated by SURF for EU/EEA Education customers.

The most important differences with Zoom’s global DPA are:

- More and expanded definitions for the different data types processed by Zoom
- Expanded audit rights
- Transparency commitments
- References to the GDPR
- Explicit prohibitions for Zoom to process personal data for personalisation, general product development, and to ask for consent from end users or any “further” or “compatible” purposes (within the meaning of Articles 5(l)(b) and 6(4) GDPR) other than those specified in the DPA or enabled by the Zoom account administrator
- Commitment to take reasonable measures to prevent malicious applications in the “Zoom Marketplace”
- Zoom agrees to only transfer pseudonymised Diagnostic Data to the USA, and to scrub any Customer Content Data from Diagnostic Data if accidentally included in logs such as SIEM logs
- In the SURF DPA dynamic information is ‘frozen’ by attaching the information as appendix to the DPA and agreeing with Zoom on procedures that put the customers in control over updates (for example the list of subprocessors, the Acceptable Use Policy, and the list of retention periods)

2.3. Agreed action plan mitigating measures

SURF did not just sign an improved data processing agreement with Zoom, but also agreed with Zoom on an action plan to implement risk mitigation measures. In June 2023 SURF published an update about the progress of these commitments, and concluded that Zoom had introduced important new privacy updates and tools for its EU Education customers.⁴⁷

⁴⁷ SURF, Zoom gives users more control and insight into their data with global privacy enhancements, 6 June 2023, URL: <https://www.surf.nl/en/zoom-gives-users-more-control-and-insight-into-their-data-with-global-privacy-enhancements>.

2.4. Zoom's change of global terms and conditions in March 2023

In August 2023, media reported that Zoom's change of its global terms and conditions would allow Zoom to analyse Content Data from customers with AI. Zoom replied that the change was misunderstood,⁴⁸ and SURF informed the education sector that these changes were not relevant for Zoom's European Education customers, as such a purpose of the data processing is not allowed in the data processing agreement.⁴⁹ Zoom has reassured SURF that the educational institutions are in control. If Zoom offers AI services, universities can decide on an opt-in basis if they want to use those (possibly third party) services.

2.5. Definitions of different types of personal data

2.5.1. 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."

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."

⁴⁸ Zoom, How Zoom's terms of service and practices apply to AI features, 7 August 2023, last updated 11 August 2023, URL: <https://blog.zoom.us/zooms-term-service-ai/>.

⁴⁹ SURF, Zoom's online terms and conditions do not affect Dutch (and European) education, 21 August 2023, URL: <https://www.surf.nl/en/zooms-online-terms-and-conditions-do-not-affect-dutch-and-european-education>.

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.”

2.5.2. Definitions Zoom

Zoom uses the following definitions and descriptions of personal data in the 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.”⁵⁰

In the 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.”⁵¹

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 admin enables Feedback submissions or when users 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 log-in, visit the Zoom website, schedule a meeting, invite guests or other paid account users to meetings. Zoom can indirectly collect personal data about every interaction with its website and cloud Meeting

⁵⁰ Zoom DPA, Clause 1.13.

⁵¹ Zoom DPA, Clause 1.2.

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*.

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

In the 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. .”⁵²*

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

⁵² Zoom DPA, Clause 1.9.

in [Appendix 1](#). In 2021 several new brief inspections were done on the Website Data, lastly on 1 February 2022. The results of these extra tests are described in more detail below.

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 most 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 has confirmed to Privacy Company that webserver access logs are stored on Frankfurt servers.

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 committed to gradually increase its transparency about the different Diagnostic Data. Zoom has since fulfilled its commitment 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.

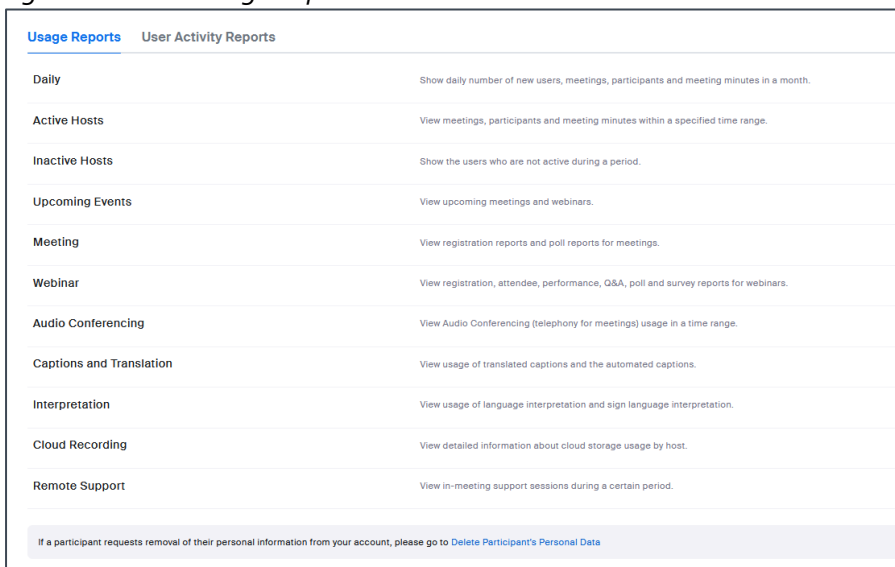
In reply to this Updated DPIA, Zoom explained that it systematically collects two types of Diagnostic Data previously not described in the DPIA: (1) the pseudonymised e-mail address and user account identifier when a user logs in and (2) the clipped IP addresses of all EU users in a separate file for US tax audit purposes only. Zoom does not provide access to these logs that are exclusively generated or stored in the USA.

Zoom explained why it needs to process the initial log-in in the United States, to ensure users are uniquely identifiable, and to be able to reroute users to their chosen geolocation (for Dutch Education customers: the EU geolocation). If Zoom would not have such a central routing system, each log-in request would have to be shared with all global geolocations to find out to what geolocation that user belongs to. That would increase the amount of international data transfers and would create latency.

With regard to the storage in the USA of IP addresses, Zoom clips the last octet of the IPv4 address, and the last 64 bits of the IPv6 address.⁵³ With IPv4, the identifiability is reduced to 1 in 255 possible users. However, not all 255 users are using Zoom. Zoom investigated whether it could further reduce identifiability by clipping the last 2 octets. However, Zoom’s legal advisors warned that that would reduce the accuracy of the mapping too much, below the 95% accuracy requirement. The IP addresses are available for admins in the audit logs, based on the processing of these personal data in the chosen EU geolocation.

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 the initial DPIA, the logs and reports were compared with the input provided through the scripted test scenarios.

Figure 10: Zoom Usage Reports⁵⁴



Usage Reports	
User Activity Reports	
Daily	Show daily number of new users, meetings, participants and meeting minutes in a month.
Active Hosts	View meetings, participants and meeting minutes within a specified time range.
Inactive Hosts	Show the users who are not active during a period.
Upcoming Events	View upcoming meetings and webinars.
Meeting	View registration reports and poll reports for meetings.
Webinar	View registration, attendee, performance, Q&A, poll and survey reports for webinars.
Audio Conferencing	View Audio Conferencing (telephony for meetings) usage in a time range.
Captions and Translation	View usage of translated captions and the automated captions.
Interpretation	View usage of language interpretation and sign language interpretation.
Cloud Recording	View detailed information about cloud storage usage by host.
Remote Support	View in-meeting support sessions during a certain period.

If a participant requests removal of their personal information from your account, please go to [Delete Participant's Personal Data](#)

As shown in Figure 10, Zoom currently provides access for admins to the following usage 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.

⁵³ Zoom is working to update the standard on clipping of IPv6 addresses to the last 80 bits.

⁵⁴ Screenshot made on 27 November 2023.

- **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.
- **Use of captions and translation:** View usage of translated captions and the automated captions. This log file contains the Meeting ID, the host email, meeting type, the start date and time of the captions, the end date and time of the captions, and the duration of the captions. In the test tenant, the translation option was not available (as this requires use of AI, and this was not enabled)
- **Interpretation:** View usage of language interpretation and sign language interpretation. This log file contains the Meeting ID, the host email, the meeting type, the start date and time of the interpretation, the end date and time of the interpretation, and the total minutes interpreted.
- **Cloud recording:** View detailed information about cloud storage information by host. This log file contains the dates of usage and the amount of data used in the cloud on each day.
- **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.
- **Zoom also provides User Activity Reports.** These reports show information from 9 different audit and activity logs:
- **Admin Activity Logs:** “Audit admin’s operation within up to a month”. These logs may be exported for time periods of one month and contain records of actions taken by administrator users. These actions include, for example, deleting user accounts or exporting data. This log file contains admin- activities, , such as a user changing her password. 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 2021.⁵⁵ Privacy Company retested this and confirmed the removal in May 2021.

- **Sign-in/Sign-out:** *“Audit user activities of sign-in and sign-out”*. These logs may be exported for time periods of one month and contain a list of user emails, times of sign in or sign out, whether the user signed in or signed out, the IP Address of the user, whether the Zoom client is in the browser or desktop, and the version of the Zoom client used. 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 Client Type (such as ‘browser’, ‘mac’, or ‘win’).
- **Chat History:** *“View your account’s Team Chat conversations”*. Users may view or download a history of chats for specific dates. This data includes the participants/group name of those in the meeting, and is available for download as a text only CSV or an HTML file including attachments and a csv. This data is provided in an encrypted ZIP file and the user is provided a four-character password for decrypting it. These files contain the headers Session Id, Sender, Receiver, Message Time (UTC), Message, Emoji, File, Giphy, Edited/Deleted, and Edited/Deleted Time (UTC). 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.
- **Channel Activity Logs:** *“View your account’s Team Chat Channel activity”*. This log contains event types such as the creation of channels and the ownership of channels, the date such action was taken, and the initiator of the action. This log contains information about activity in an organization’s Team Chat conversations. The logs contain records of the creation of chats, chat membership, chat ownership, the settings and permissions for chats, and a final category entitled “other”.
- **Legal Hold for Team Chat:** *“Create and view legal holds on specific individuals/users, for regulatory compliance purposes”*. These logs store revisions to edited and deleted messages if the feature is enabled in the Team Chat Settings.
- **Disclaimers:** *“View information about disclaimers shown when users sign in, join meetings/webinars, and start recordings”*. These logs contain the user, the type of disclaimer, the status of the disclaimer, the type of client, the time, and the Meeting ID. 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 portal. The admin can use this disclaimer to show

⁵⁵ Ibid.

information about the organisation or show behavioural rules. This log shows the disclaimer type and status of users within up to a month.

- **Reported Participants:** *“View the participants you’ve reported before”*. These logs contain three types – reports waiting for confirmation by the user, confirmed reports, and completed reports. A user filing a report may label the report as one of the following categories – Submit a Law Enforcement Request, Report Abusive Behavior or Content, Report Account Compromise, Report Fraud, and finally Report Copyright or Trademark infringement.
- **Attendee Logs:** *“View the meetings and webinars a user has joined, both as a host and a participant. These logs contain the name of attendees, the emails of attendees”, Meeting IDs, the topic of a meeting, the host of a meeting, the name of the account of the host of the meeting, the number of meeting participants, the start and end times of a meeting, the status of whether a user has joined a meeting, the time at which a user joined a meeting, the time at which a user left a meeting, and whether a user has used the features screensharing, file sharing, recording, video, phone, VOIP, or chat. It also contains whether or not a meeting was End-2-End-Encrypted and if the meeting was internal to an organization.*
- **Requests of accessing content:** *“View the requests of accessing your Zoom content”*. These logs include the categories of pending requests, approved requests, and denied requests.

Figure 11: Zoom User Activity Reports⁵⁶

Usage Reports	User Activity Reports
Admin Activity Logs	Audit admins' operation within up to a month.
Sign In/Sign Out	Audit user activities of sign-in and sign-out.
Chat History	View your account's Team Chat conversations.
Channel Activity Log	View your account's Team Chat Channel activity.
Legal Hold for Team Chat	Create and view legal holds on specific individuals/users, for regulatory and compliance purposes.
Disclaimers	View information about disclaimers shown when users sign in, join meetings/webinars, and start recordings.
Reported Participants	View the participants you've reported before.
Attendee Log	View the meetings and webinars a user has joined, both as a host and participant.
Requests of accessing content	View the requests of accessing your Zoom content.

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

⁵⁶ Screenshot made 27 November 2023.

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.”*⁵⁷

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 updated Privacy Data Sheet, under Meeting and Webinar Participant Information.⁵⁸

Additionally, Zoom has added the 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.

3.2. Telemetry Data

Zoom does not (yet) offer any tools similar to the Data Viewing Tool provided by Microsoft or Diagnostic Information Tool provided by Google for end-users to see what Telemetry Data have been sent from their apps. Nor does Zoom yet provide a separate log with the Telemetry Data that are automatically sent to Zoom from Zoom apps installed on the end-user devices in reply to a DSAR request. These logs are currently mixed with other logs in many different files. Zoom has implemented the telemetry toggle for admins (to enable them to opt-in to Optional Telemetry events) on 16 December 2023.⁵⁹ See [Figure 12](#) below.

Zoom has confirmed to SURF that it is only collecting required telemetry as the default option. *“By default, Zoom does not collect Optional telemetry from users in Dutch education and Enterprise accounts. Here are the final numbers for our Meetings, Webinars, and Team Chat telemetry events for Zoom desktop client and mobile app version 5.17.0:*

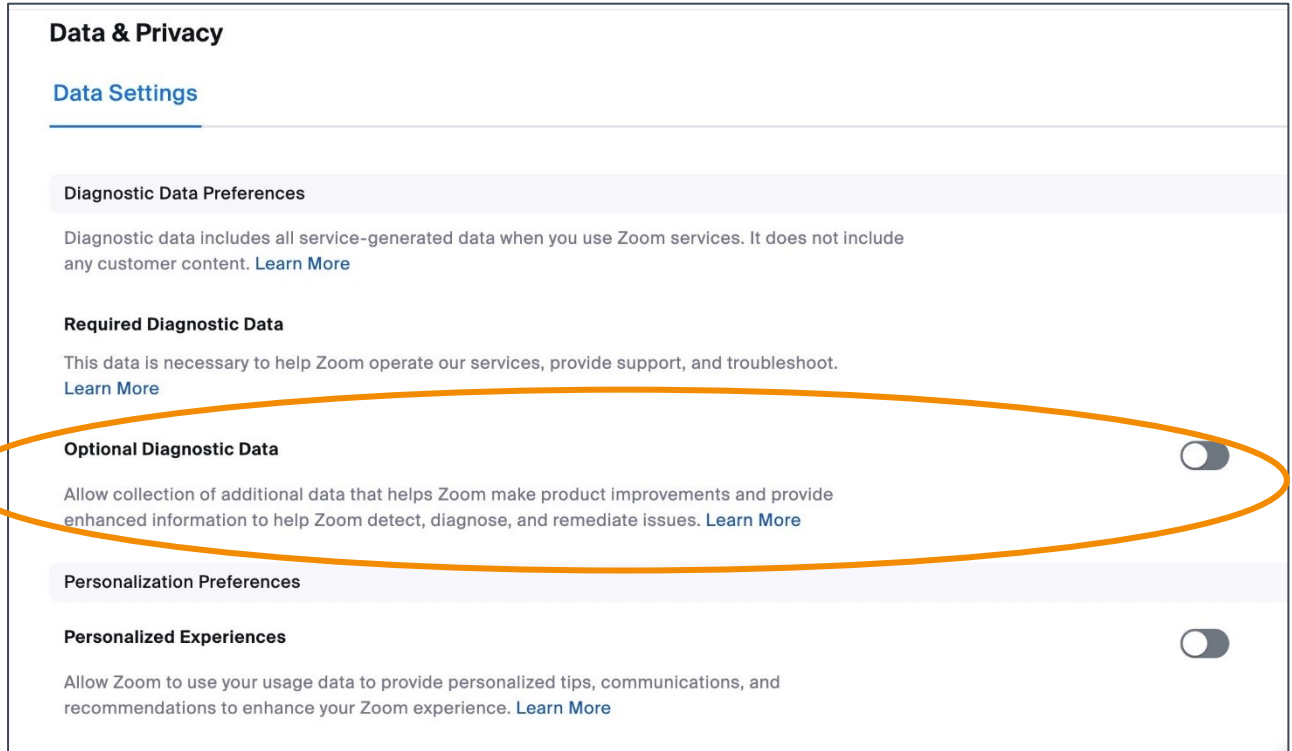
⁵⁷ Zoom reply to part A of the DPIA, 19 March 2021, p. 29.

⁵⁸ Zoom, Privacy Data Sheet, last updated April 2023, URL: <https://explore.zoom.us/media/privacy-data-sheet.pdf>.

⁵⁹ Zoom, What data is included in “Optional Usage & Diagnostic Data”, last updated 23 August 2023, URL: <https://community.zoom.com/t5/Billing-Account-Management/What-data-is-included-in-quot-Optional-Usage-amp-Diagnostic-Data/m-p/130726>.

- *Total Meetings, Webinars, and Team Chat events: 746*
 - *Required Meetings, Webinars, and Team Chat events: 19*
 - *Optional Meetings, Webinars, and Team Chat events: 727.*⁶⁰

Figure 12: Screenshot new Telemetry toggle (since 16 December 2023)



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. In November 2023, Privacy Company performed a short re-test and captured the Telemetry Data sent from a Windows and an Android test device. The results were the same as in 2020.

⁶⁰ E-mail Zoom after confidentiality review of this Update DPIA.



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

The first example (from MacOS, captured in 2020) contains two events sent to the URL: <https://eu01logfiles.Zoom.us/stat/append/3bdDCvtUdtgM7X%2BuLZf79WIDlu7jTmLQ2YNzdDLgl7A%3D>.

Figure 13: 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":"focAptkITTSfHTiULJWSlw=",
  "sub_event": "",
  "user_id":"6n1pCAW4TT2qj5tmnGoKSg",
  "uuid":"3bdDCvtUdtgM7X uLZf79WIDlu7jTmLQ2YNzdDLgl7A="
}
{
  "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 uLZf79WIDlu7jTmLQ2YNzdDLgl7A="
}....

```

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, not in 2020 and not in 2023. The events also did not contain information about other users, meeting names or other user-supplied values such as profile names.**

Figure 14: Another telemetry example from Zoom on Windows (28 November 2023)

```
{
"client_os":"win7",
"client_type":"Zoom Main Client",
"client_version":"5.16.6.24712",
"event":"Adjust Settings",
"event_loc":"In Meeting",
"event_time":"11/28/2023 12:38:17",
"sub_event":"UnMute",
"user_id":"UXC4m21rQDyApsdJR8Vm7g",
"uuid":" t8NvvR8dbkgLXzog3zkyaLIEnICsO1SPIXmI5jIPKQ="
}
```

Zoom has used these observations to improve its public documentation, and confirms these findings in a help article about the Telemetry Data.⁶¹

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.

Amount of Telemetry events

Currently, Zoom describes the collection of 746 different telemetry events for Meetings, Webinars and Team Chat events. In the technical test in 2020, in total 240 telemetry (often identical) events were observed in the outgoing network traffic from the 5 tested platforms and 2 plug-ins, resulting in 42 observed unique events. Zoom at the time confirmed it collected a maximum of 49 unique telemetry events about Meeting, Webinar and Chat. Currently, Zoom describes it collects 19 unique required telemetry events for these 3 tested services. This is a very low number, compared to other telemetry streams collected by cloud providers (as inspected by Privacy Company for other DPIA

⁶¹ Zoom, Zoom Meeting, Webinar, and Team Chat Telemetry Events, 1 March 2024, URL: https://support.zoom.com/hc/nl/article?id=zm_kb&sysparm_article=KB0074458.

reports). The contents of these telemetry events are unsurprising, with the exception of the UUID and UID. Zoom confirmed the amount of required telemetry events related to the use of the Meeting, Webinar, & Chat services is only a small portion of the total of 746 unique telemetry events, as 727 events belong to the category of optional telemetry events.

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. Zoom now also explains this data collection in the Privacy Data Sheet and in more detail, in the help article about the Telemetry Events.

Based on the technical analysis and the 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 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 has fulfilled its commitment to build a tool for admins to easily export all Diagnostic Data relating to a specific user, but did not yet deliver the agreed do-it-yourself take out tool for users.

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."⁶²

⁶² Zoom new DPA.

Privacy Company initially filed DSARs in 2020 and compared these outputs with the results of the use of the new export tool in November 2023.

Results DSAR in 2020

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 replied by e-mail the same day with a reference to the information available in-product for users and in the console for Zoom administrators.⁶³

On 13 November 2020 Zoom provided a substantial response to the two 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. This prevented Zoom from providing access to Website Data.
- 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.

The output also included information with regard to Zoom's websites and the use of cookies. Zoom did not provide access to its webserver access logs, with the following explanation: *"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 not available in an identifiable fashion. Thus, we cannot provide any information pursuant to your request for these third parties."*⁶⁴ Zoom also provided information what cookies it used, from what third parties. Zoom has since developed a cookie policy and implemented a cookie consent banner (see Section 3.4 below).

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

⁶³ 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."

⁶⁴ Zoom response to DSAR, 13 November 2020.

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.

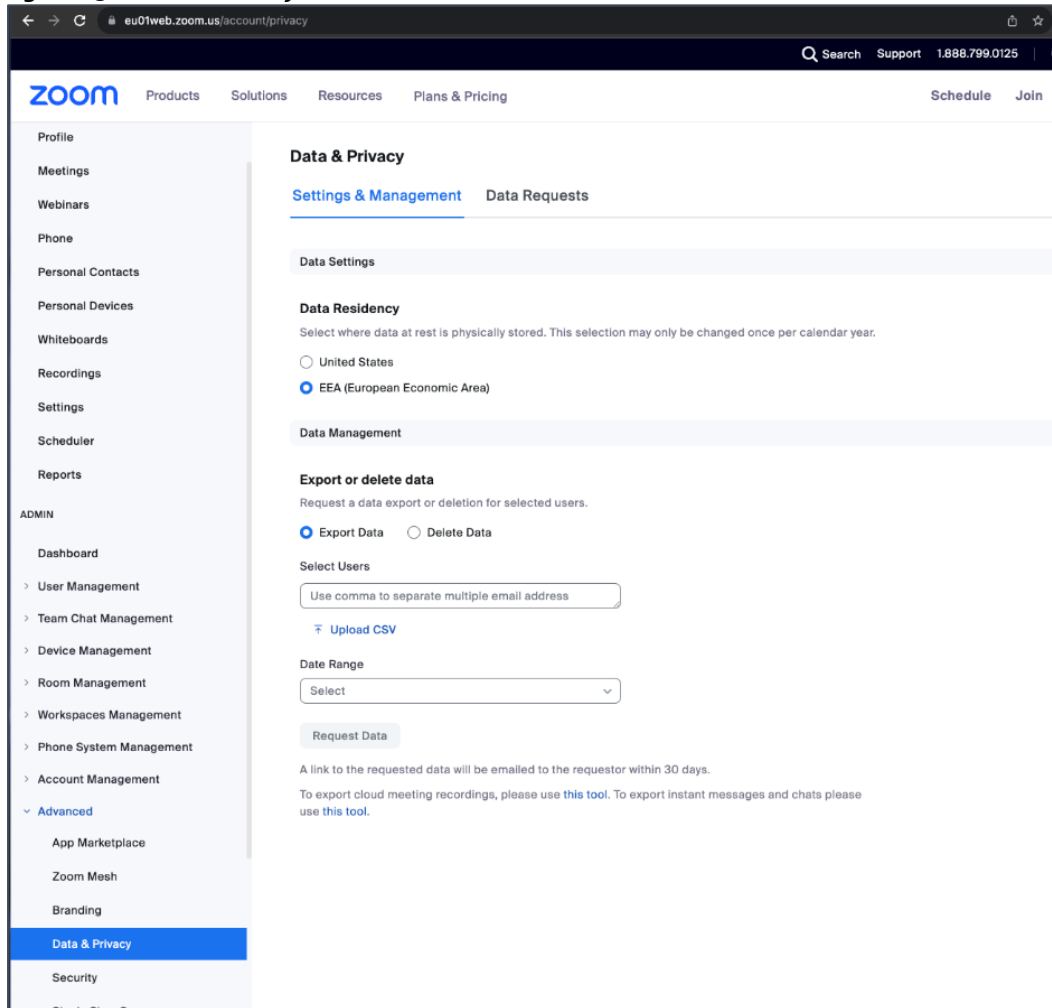
Results DSAR in 2023

As mentioned at the start of this paragraph, Zoom has become a data processor (factually and contractually, with the 2022 DPA) for all personal data, except for the public Website Data.

On 6 June 2023, Zoom announced it would enable admins to respond to end user Data Subject Access Requests, and that users have do-it-yourself access to the marketing settings via the Marketing Preference Center: *“Zoom’s new tools for data subject access requests and data deletion are available in the Zoom web portal, under “Privacy.” The Marketing Preference Center can also be accessed through the “Manage Preferences” link within Zoom marketing emails”, and European technical support is also available at <https://eu.support.zoom.us>. For EEA-based paid customers, Zoom also began rolling out the ability to enable EEA-based data storage in the Zoom Privacy Center.”*⁶⁵

⁶⁵ Zoom, Zoom Gives Users More Control and Insight Into Their Data with Global Privacy Enhancements, last updated 6 June 2023, URL: <https://news.zoom.us/zoom-gives-users-more-control-and-insight-into-their-data-with-global-privacy-enhancements/>.

Figure 15: Data & Privacy menu available to account owners

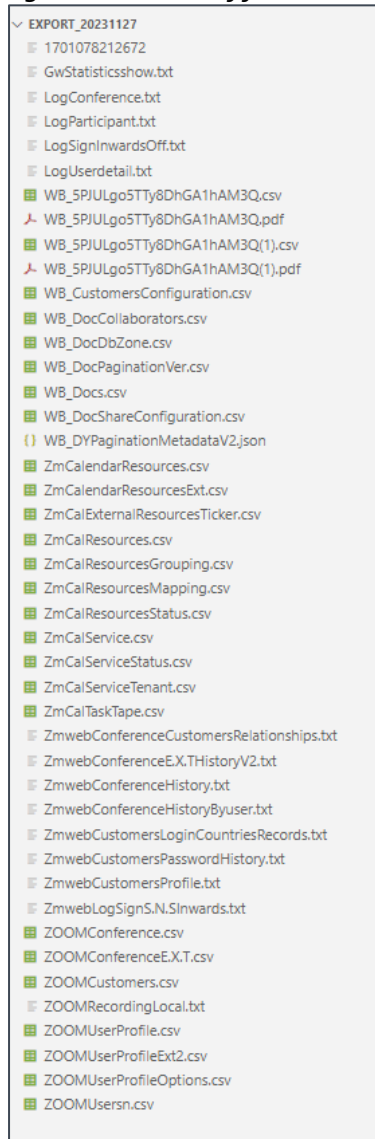


In the statement quoted above, Zoom describes a “Privacy” web portal. This web portal, pictured above, is accessible for account owners (not end users) and is entitled “Data & Privacy”⁶⁶.

This portal allows account owners to export or delete data for specific users within a specified date range. For this Update DPIA, Privacy Company requested data through this tool and received the data on 27 November 2023. [Figure 16](#) below shows the names of the files returned through this request.

⁶⁶ Last checked 17 November 2023.

Figure 16: The list of files returned through the self-service DSAR tool



The different files provided by Zoom are listed below. The file did not contain a readme document explaining the meaning of each file, but Privacy Company provides an explanation of the contents where possible. The output did not contain a separate map with ‘event logs’ about the Telemetry Data. In dialogue with Zoom, in January 2023, Zoom explained it purposefully created meaningless names for the files, and mixer data from different log files in these DSAR results, to prevent disclosing company confidential infrastructure that could be abused for reverse engineering by malicious actors.

Zoom acknowledged that randomizing table names/file names for security reasons is not helpful for people to file a DSAR request to understand what data Zoom processes about them. Zoom agreed to improve the understandability of the output, by grouping the output by product in a more accessible

file, as well as improving the current Help article about the Data & Privacy menu. Zoom honoured both commitments prior to the completion of this Update DPIA: by publishing the expanded information about each file in the DSAR results on 27 February 2024⁶⁷ and by providing a more understandable output, grouped by product.⁶⁸ Zoom will also make a new Do It Yourself access tool available for end users before the end of 2024.

The explanations below are a combination of descriptions from Privacy Company, and the new descriptions provided by Zoom.

- GwStatisticsshow.txt: -contents were unclear, but Zoom now explains: *“Contains meeting and webinar information such as attendee information, and meeting information such as meeting ID and quality of service.”*
- LogConference.txt: This file contains Diagnostic Data relating to Zoom conferences. Among other data types, it includes the full name of the Account Owner (super admin) whether the conference used end to end encryption, the number of participants, the Tenant ID, and the user ID of the account owner.
- LogParticipant.txt: This file contains Diagnostic Data relating to participants in Zoom meetings. Among other data types, it includes the unique identifier of the client, the full name of the participant, information about the device used during the meeting, the name of the device being used by the participant (for example “First Name last name’s MacBook Pro), the meeting ID, whether the user is using encryption, the IP address of the participant, and the email of the participant.
- LogSignInwardsOff.txt: This file contains Diagnostic Data relating to participants log in and log out events. Among other data types, the file contains the email of the user, the tenant ID, the channel through which the user logged in or logged out, and the time of the events.
- LogUserdetail.txt: This file contains, among other data types, a log of account IDs and meeting IDs.
- ZmwebConferenceHistory.txt: This file contains a log of Zoom conference calls. Among other data types, it includes the ID of the conference, the email address of the account owner, the user ID of the account owner, the name of the account owner, the topic of the Zoom meeting (example First Name Last Name’s Zoom Meeting), the date and time of the beginning of the conference, and the stop time of the conference.

⁶⁷ Zoom, Using Data & Privacy for data management, 27 February 2024, URL:

https://support.zoom.com/hc/en/article?id=zm_kb&sysparm_article=KB0057736

⁶⁸ Zoom mailed a sample of the new DSAR output on 27 February 2024.

- ZmwebConferenceHistoryByuser.txt: This file contains a record of conferences in which a user participated. Among other data types, it includes the full name of the user, the tenant ID, the email of the user, and the date of the conference.
- ZmwebCustomersLoginCountriesRecords.txt: This file contains a record of user log in without user ID's. Among other data types, it contains the country from which the user logged in, the software agents from which the user logged in, the IP address of the log in, the date and time of the login, and whether the user logged in from the web or desktop client. See [Figure 17](#) below.

Figure 17: Example of CustomersLoginRecords.txt

```
{
  "Customers IDs": "6n1pCAW4TT2qj5tmnGoKSg",
  "S.N.S Kind": 100,
  "TimeToLive": 1699607867,
  "Countries": "NL",
  "Customers Agents": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/117.0.0.0 Safari/537.36",
  "Log in From": "web",
  "Log in Appointment": "2023-10-11 09:17:47",
  "IPs": "185.213.106.92"
}
```

- ZmwebCustomersPasswordHistory.txt: This file contains a record of when a user updated his or her password. It contains the time and date of the update, the customer Id, and the tenant ID.
- ZmwebCustomersProfile.txt: This file contains the Customer (i.e., user) ID, the Tenant ID, and a date and time labelled “Update Time” representing the creation of a Zoom profile.
- Zmwebl.MUsage.txt: This file contains entries with the values representing the presence of different media types in calls, such as Images, Text, Sound, or End to End encrypted messages.
- ZmwebLogSignS.N.SInwards.txt: This file contains information about user log ins to the web client. Among other data types, it includes a Device uuid, the version of Zoom used, the name of the device used to log in, the name of the user logging in, the tenant ID, the user ID of the user logging in, and the email of the user logging in.
- ZmwebOpAuditLog.csv: This csv file contains rows tracking certain user activities, along with the email address of the user who did the activity and the date and time of the activity. In the data received by Privacy Company, these activities were “loginWeb” and “freeTrialUpgradeFreeAccount”.
- ZmwebWebinarE.X.T.txt: This file contains records relating to webinars, including the topic of the webinar, the date and time of the webinar, and the agenda of the webinar.

- ZOOMConference.csv: This file contains records relating to Zoom conferences. Among other data types it contains the topic of the conference and information relating to the date and time of the conference.
- ZOOMCustomers.csv – part of Zoom Core processing, with the description: *“Information related to user and account settings including user names, email address and billing address.”*⁶⁹
- ZOOMMimo.csv – related to the use of Zoom Rooms
- ZOOMTenant.csv - part of Zoom Core processing, with the description: *“Information related to user and account settings including user names, email address and billing address.”*
- ZOOMUserProfile.csv – idem
- ZOOMUserProfileE.X.T.csv - idem
- ZOOMUserProfileExt2.csv -idem
- ZOOMUserProfileOptions.csv -idem
- ZOOMUsersn.csv – idem
- ZrcoRoom.csv – *“Zoom Rooms device management which will include information such as device name, device model and account ID.”*

In sum, the contents of the log data did not contain any surprising details, but the obfuscation of the file names and the lack of explanation made it too difficult for recipients to understand the answer to their DSAR request. Privacy Company and SURF will perform a retest after Zoom has implemented the agreed improvements.

In addition to the DSAR request, Zoom provides the owner account with a tool to keep track of the status of requests made for the data of different users within an organisation.

⁶⁹ Information in the new table with descriptions of exported user data, in Zoom, Using Data & Privacy for data management, URL: https://support.zoom.com/hc/nl/article?id=zm_kb&sysparm_article=KB0057736.

Figure 18: Tool for account owners to track data subject requests

The screenshot shows the 'Data & Privacy' section with a 'Data Requests' tab selected. A search bar is present with the text 'Search by email' and an 'Advanced Search' dropdown. Below is a table with columns: Request Date, Email(s), Requestor, Request Type, Data Types, Date Range, Status, and a 'Download' button. The table contains 8 rows of request data.

Request Date	Email(s)	Requestor	Request Type	Data Types	Date Range	Status	
11/03/2023 01:54:29 PM	floorterra@privacycompany.nl	Floor Terra	Export Data	All Data	11/03/2022 - 11/03/2023	Completed	Download
03/08/2023 04:49:51 PM	sjoera.nas@privacycompany.nl	Floor Terra	Export Data	All Data	03/01/2023 - 03/08/2023	Completed	Expired
03/08/2023 08:35:38 AM	frank.koppejan@privacycomp	Floor Terra	Delete Data	All Data	-	Completed	Expired
03/07/2023 10:56:23 AM	sjoera.nas@privacycompany.nl	Floor Terra	Export Data	All Data	02/28/2023 - 03/07/2023	Completed	Expired
03/07/2023 09:35:58 AM	winfried.tilanus@privacycomp	Floor Terra	Export Data	All Data	03/07/2022 - 03/07/2023	Completed	Expired
03/06/2023 07:53:45 PM	sjoera.nas@privacycompany.nl	Floor Terra	Delete Data	All Data	-	Completed	Expired
03/06/2023 07:51:37 PM	floorterra@privacycompany.nl	Floor Terra	Export Data	All Data	03/06/2022 - 03/06/2023	Completed	Expired
03/03/2023 09:25:08 AM	sjoera.nas@privacycompany.nl	Floor Terra	Export Data	All Data	02/01/2023 - 03/03/2023	Completed	Expired

At the bottom, there is a pagination control showing '15/page' and '8 results'.

Finally, the owner has the ability access a log of when administrators have taken actions using the DSAR tool. During testing, Privacy Company used an administrator account and an account that acted as both owner and administrator. Only the owner administrator account had access to the Data and Privacy menu and the ability to export or delete data.

Figure 19: The tool provided to owner accounts for tracking administrator use of DSAR tools

The screenshot shows the Zoom Admin Activity Logs interface. The breadcrumb trail is 'Reports > User Activity Reports > Admin Activity Logs'. There are search filters for 'From' (2023-11-02) and 'To' (2023-11-03), a search bar 'Search by target email', and dropdowns for 'All Categories' and 'All Actions'. A 'Search' button and an 'Export' button are also visible. Below the filters is a table with columns: Time, Operator, Category, Action, and Admin Activity Detail. One row is visible with the following data:

Time	Operator	Category	Action	Admin Activity Detail
2023-11-03 13:54:29	floorterra@privacycompany.nl	Privacy	Export Data	Export data: 1 email(s)

Navigation arrows are present at the bottom of the table.

If end users want to file a DSAR for personal data processed by Zoom as controller (very limited data relating to the public Website Data) they can use a separate web portal.⁷⁰ This portal is created and managed with the company OneTrust.

Figure 20: DSAR form when Zoom is data controller

zoom

Data Subject Rights Request Form

Please use this form to submit a data subject request.

Instructions: To exercise any of your rights as to personal data controlled by Zoom, please follow the instructions below.

1. Please complete this form with all relevant information. For information on Zoom's account types or plans, please click [here](#).
2. This form will be sent directly to the Privacy Team.
3. You will receive an automated email requiring authentication.
4. The Privacy Team will investigate and respond in accordance with regulatory requirements.

If you are a **Member** of a Pro, Business, or Enterprise (paid) account, please contact your **Account Owner** to exercise your data subject rights.

If you are an **Account Owner** intending to submit a data subject request on behalf of a **Member** of your account, please refer to the following articles on Zoom Support: [Using Privacy for data management](#), [Deactivating, unlinking, or deleting users from your account](#), and [Getting started with Zoom reporting](#).

To understand the personal data Zoom collects and/or processes, please refer to the [Zoom Privacy Statement](#).

* I am a

This field is required

* First Name

This field is required

* Last Name

This field is required


* Country of Residence

This field is required

* Email Associated with Zoom Account

This field is required

By agreeing to submit a request via this form, you understand that Zoom will process your information to authenticate your identity and respond to your data subject access request.

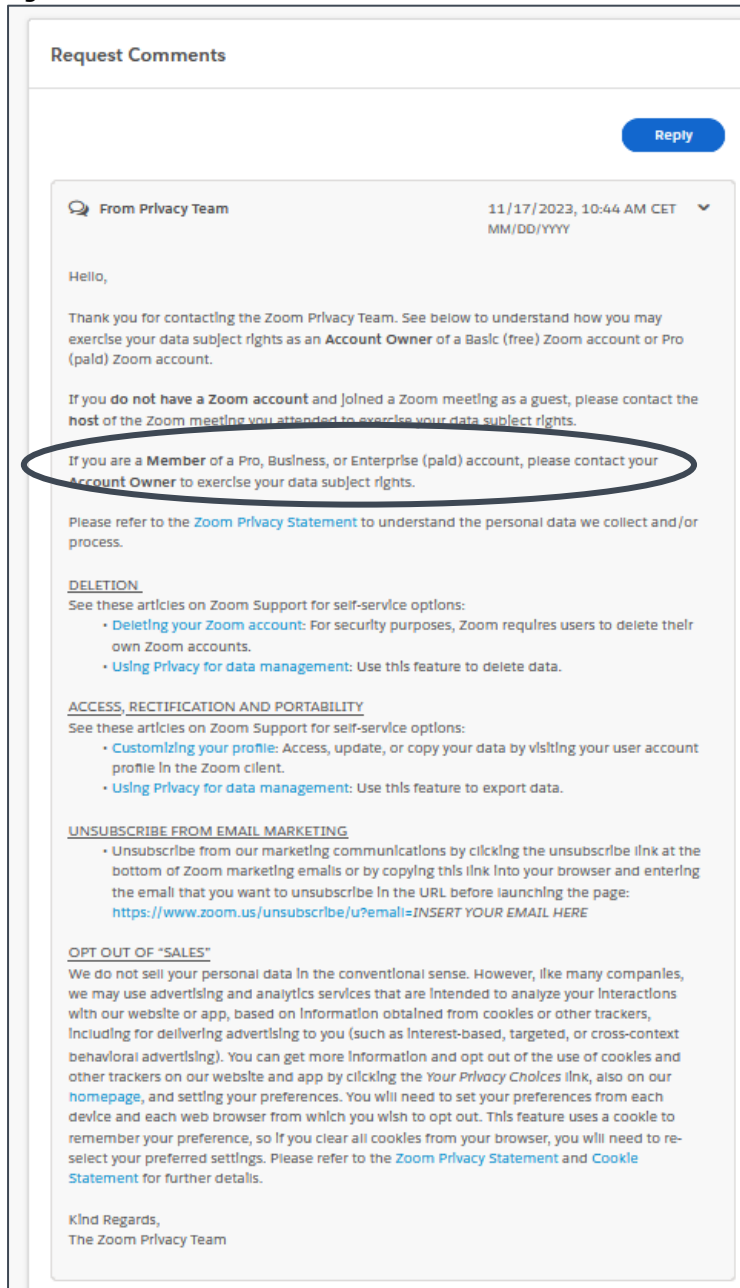
I'm not a robot 

Submit

⁷⁰ Zoom, Data Subject Rights Request Form, last viewed 17 November 2023, URL: <https://zoom-privacy.my.onetrust.com/webform/65962359-ef0d-4399-9db4-572d06de08aa/f277f9f7-bfee-4233-815e-80e290139bc2>.

The form is aimed at consumer users and enables users to exercise different data subject rights when Zoom acts as data controller: to “Receive my information”, “Delete my information”, “Update or correct my information”, or to “Opt-out of sales”.

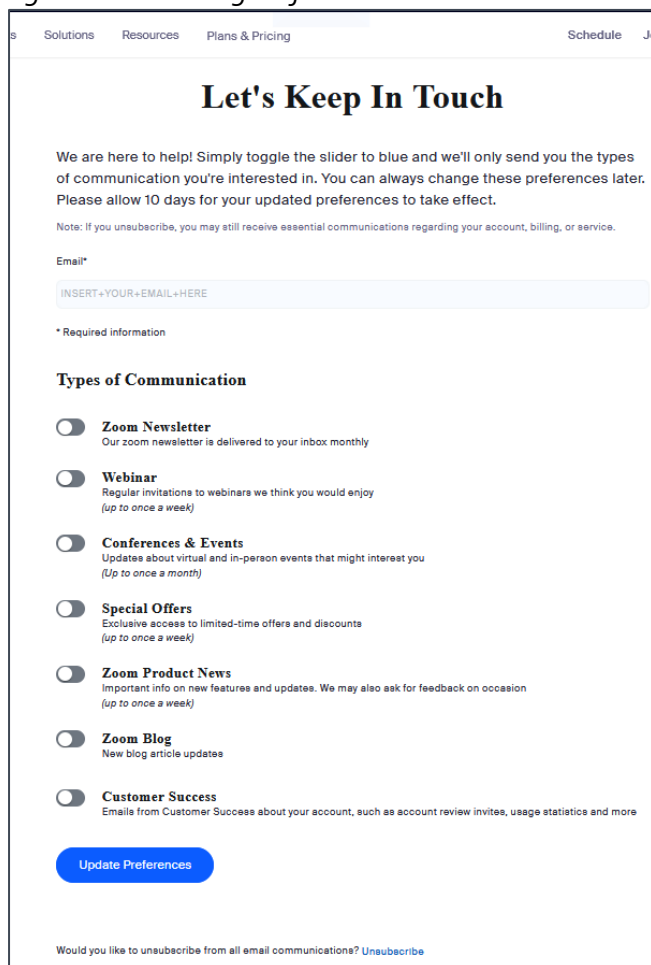
Figure 21: Zoom instruction to contact the account owner



The form includes a message informing end users that are not account owners that they have to ask their account owner (education or research organisation) to exercise their data rights. Zoom also provides guidance to account owners about the Data and Privacy menu.⁷¹

Privacy Company tested in November 2023 what happened if a user enrolled in an EU Education tenant filed this form. Zoom sent a message with the request to confirm the user’s identity at the email associated with the Zoom account. After this confirmation, Zoom gave access to a OneTrust portal but also immediately sent a prewritten message informing the user to contact their account owner to exercise their data subject rights.

Figure 22: Marketing Preferences menu



The screenshot shows a web page titled "Let's Keep In Touch" with a navigation bar at the top containing "Solutions", "Resources", "Plans & Pricing", "Schedule", and "Join". The main heading is "Let's Keep In Touch". Below the heading, there is a paragraph: "We are here to help! Simply toggle the slider to blue and we'll only send you the types of communication you're interested in. You can always change these preferences later. Please allow 10 days for your updated preferences to take effect." A note follows: "Note: If you unsubscribe, you may still receive essential communications regarding your account, billing, or service." There is an "Email*" field with a placeholder "INSERT+YOUR+EMAIL+HERE". Below this is a section titled "Types of Communication" with several toggle options: "Zoom Newsletter" (Our zoom newsletter is delivered to your inbox monthly), "Webinar" (Regular invitations to webinars we think you would enjoy (up to once a week)), "Conferences & Events" (Updates about virtual and in-person events that might interest you (Up to once a month)), "Special Offers" (Exclusive access to limited-time offers and discounts (up to once a week)), "Zoom Product News" (Important info on new features and updates. We may also ask for feedback on occasion (up to once a week)), "Zoom Blog" (New blog article updates), and "Customer Success" (Emails from Customer Success about your account, such as account review invites, usage statistics and more). At the bottom of this section is a blue "Update Preferences" button. At the very bottom of the page, there is a link: "Would you like to unsubscribe from all email communications? [Unsubscribe](#)".

⁷¹ Zoom, Using Data & Privacy for data management, last updated 27 October 2023, URL: https://support.zoom.com/hc/en/article?id=zm_kb&sysparm_article=KB0057736.

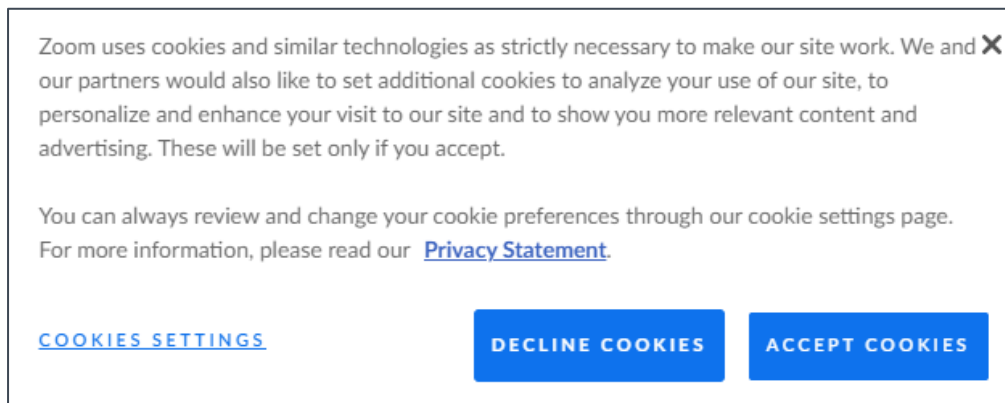
Privacy Company also tested Zoom’s new self-service tool to change marketing preferences⁷² (see [Figure 22](#) above), even though Zoom by default never sends commercial communications to admins and end users in an EU Education tenant. Based on the DPA, Zoom may only send marketing mails to its commercial contacts (Account Holder Business Data). These relations can use a general opt out, while end users have to opt-in to different types of commercial email. SURF and Zoom have contractually agreed that Zoom will never prompt or invite end users to opt-in. During the 2-year testing period, the Privacy Company test accounts never received such commercial messages.

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 in November 2021, and since 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 23](#) below.

Figure 23: Zoom Cookie Consent Manager⁷³

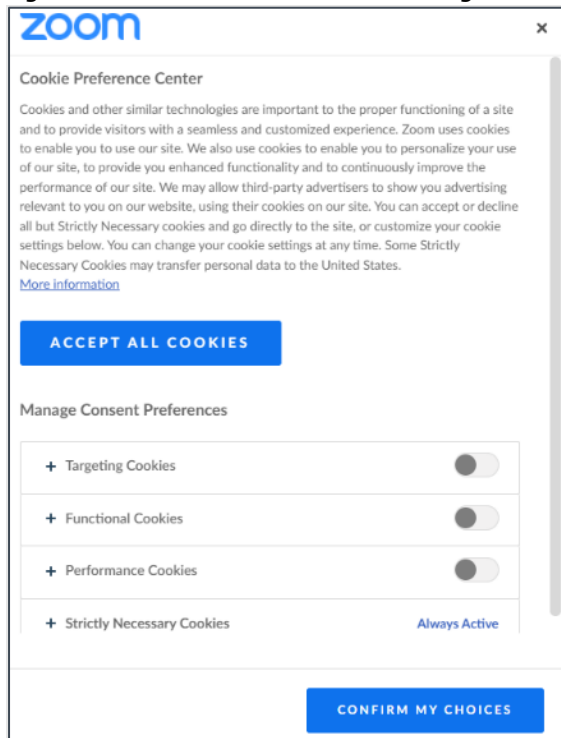


As a result of the discussions with SURF, Zoom has changed the default settings for visitors from the EU to both websites to only set and read strictly necessary cookies. See [Figure 24](#) below. Zoom has contractually committed to continue to monitor and apply this policy in the future. Zoom recognises the origin of its Website visitors based on their IP addresses.

⁷² Zoom Marketing Preferences, URL: <https://www.zoom.us/unsubscribe/u?email=INSERT YOUR EMAIL HERE>

⁷³ Screenshot 2 February 2022.

Figure 24: Zoom default cookie settings for EU visitors⁷⁴



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 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 about the NID cookies 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.

⁷⁴ Screenshot 2 February 2022.

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, even though 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 reCAPTCHA 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.”*⁷⁵

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 24](#) 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, and Zoom is a data controller for its public website. This means visitor IP addresses plus information about visited pages 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 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.

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 the preference menu for the cookies-up make visitors aware of this necessary transfer of personal data to the USA (See the highlighted text in [Figure 24](#) above) .

Privacy Company verified in November 2023 that Zoom has limited the use of cookies by subprocessors in the service provided to Dutch education and research organisations. Privacy Company tested cookies for 3 types of users: (1) an administrator who visits the Admin Console, (2) a

⁷⁵ Zoom, Cookie Statement, last updated 30 June 2023, URL: <https://explore.zoom.us/en/cookie-policy/>.

logged-in user or guest user who wishes to participate via browser and (3) an unauthenticated user who wants to look up some help information or read legal documentation on eu01web.zoom.us.

No cookies are set for which consent is required in any of the 3 scenarios. Privacy Company noted the transfer of IP address, URL referrer and User Agent to Optimizely. Optimizely does not set cookies, and for this reason it is clear why Optimizely is not listed in the Cookie Consent Manager. However, Optimizely is a third party collecting personal data, and is not mentioned in the Privacy Policy. Use of Optimizely for geolocation of users is defensible as necessary, but must be transparent. While Zoom’s framework for cookies is good, Zoom should continue to verify the labels of cookies from its consent management tool into the future to ensure that users are properly informed.

Figure 25 Cookies on Zoom home page (3 November 2023)

The screenshot shows the Zoom website at eu01web.zoom.us with a cookie consent banner. The Chrome DevTools Application tab is open, displaying a list of cookies. The cookies table is as follows:

Name	Value	Domain	Path	Expires / Max-Age	Size	Http...	Secure	SameSite	Partition ...	Priority
OneTrustActiveGroups	C00...	zoom.us	/	2024-11-02T12:55:55...	25		✓			Medium
_zm_cdn_blocked	unlo...	zoom.us	/	2023-11-03T18:55:54...	26		✓			Medium
cred	1F5...	eu01web.zoom.us	/	Session	36		✓			Medium
_zm_page_auth	eu0...	zoom.us	/	Session	42		✓	None		Medium
cdn_detect_result	ena...	eu01web.zoom.us	/	2023-11-03T12:57:54...	23					Medium
_zm_currency	EUR	zoom.us	/	2023-11-04T12:55:53...	15		✓			Medium
OptanonConsent	lsG...	zoom.us	/	2024-11-02T12:55:55...	315			Lax		Medium
_cf_bm	yRR...	eu01web.zoom.us	/	2023-11-03T13:25:53...	152		✓	None		Medium
_zm_csp_script_nonce	XI2...	zoom.us	/	Session	42		✓	None		Medium
_zm_rtk_guid	7c3...	zoom.us	/	2024-12-07T12:55:53...	44		✓	None		Medium
_zm_visitor_guid	7c3...	zoom.us	/	2024-11-02T12:55:53...	48		✓	None		Medium
_zm_lang	en-US	zoom.us	/	2024-11-02T12:55:54...	13		✓			Medium
_zm_ssld	eu0...	zoom.us	/	Session	37		✓	None		Medium

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 customers in the context of Zoom Meetings. However, this report aims to help the education and research 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 an education and research organisation with a high level of sensitivity, or sensitive if it concerns a minor.

Organisations should be aware that the names of Zoom Rooms and meetings appear in the log files. It is therefore prudent for education and research 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.

In the initial tests, Zoom also enabled admins to apply user categorisation labels. Privacy Company tested with labels such as 'boss'. This option was no longer available in November 2023. Zoom has confirmed this feature was removed in 2023.

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.⁷⁶

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 education and research 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 education and research 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

⁷⁶ Amongst others, the categories of classified information are defined in the Voorschrift Informatiebeveiliging Rijksdienst – Bijzondere Informatie (VIR-BI).

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 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.⁷⁷ In order to facilitate the exercise of Data Subject Access Requests, Zoom has developed a tool for admins to take out all data relating to a specific user. 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. To monitor lawful use of this tool, Zoom also makes audit logs available about admin behaviour.

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."*⁷⁸ 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

⁷⁷ Zoom, Attendee attention tracking, last updated 15 December 2021, URL: <https://support.zoom.us/hc/en-us/articles/115000538083-Attendee-attention-tracking>.

⁷⁸ 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>.

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.⁷⁹

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).

Similarly, employees can exchange files with special categories of data. University employees can for example 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).

⁷⁹ These specific exceptions lifting the ban on the processing are listed in Article 9(2) under a, e, and f of the GDPR.

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 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 education or research organisation. Examples are employees of other universities. 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 an education or research 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 Education license, Zoom guarantees in the new DPA that their personal data are protected under the negotiated data protection guarantees for the education and research 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 5 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. blocking participants from third countries when they host a Meeting
5. 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 26: Permissions required in the Android Meetings app⁸⁰

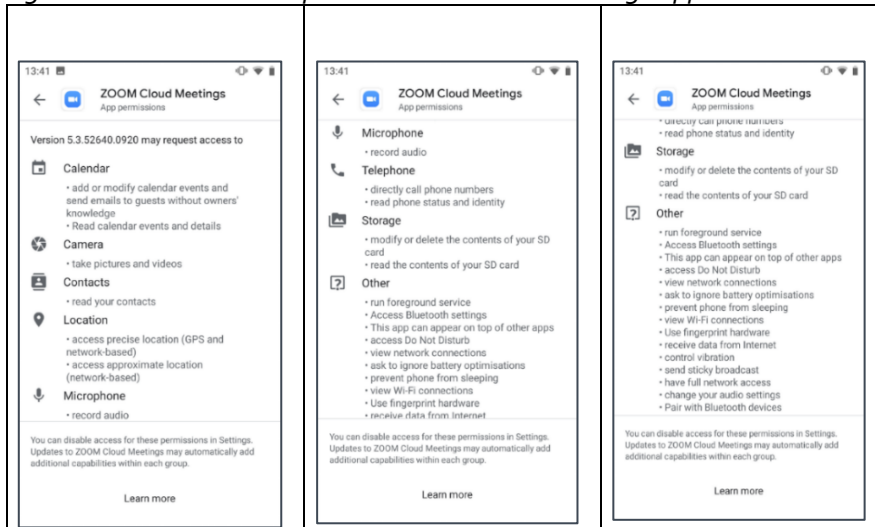
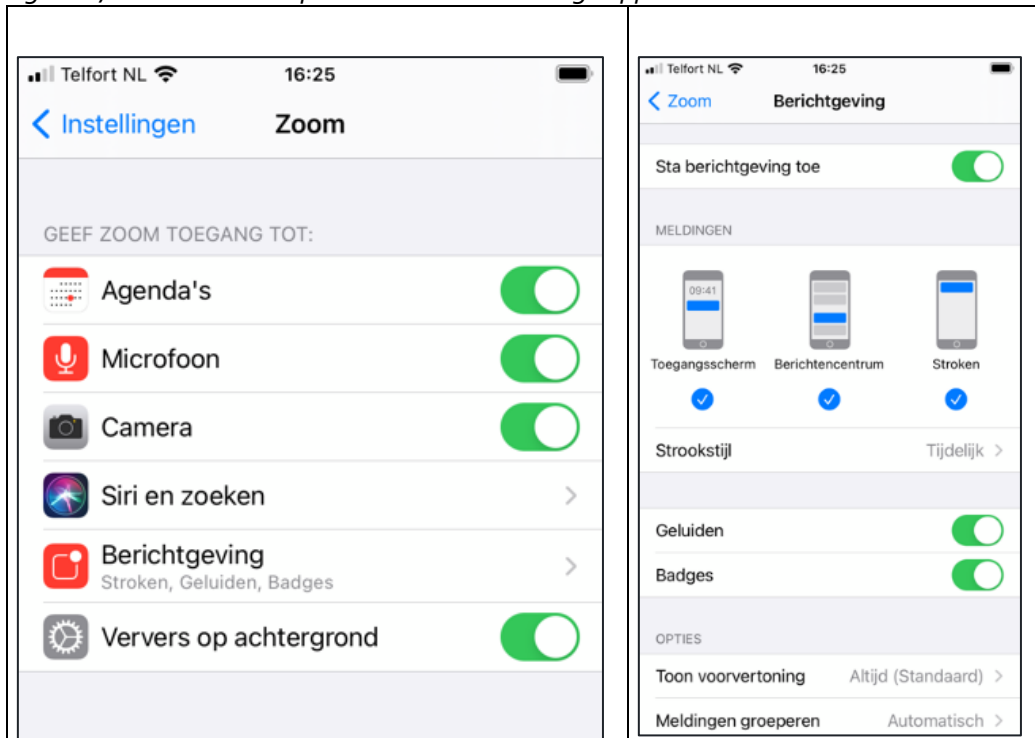


Figure 27: Permissions required in the iOS Meetings app



⁸⁰ 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.⁸¹ In this Section only some privacy options are listed. They have the following default settings:

- Enable E2EE in Account Settings – Meeting- Security (default Off)⁸²
- 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 Education customers. This was default On for end-users but default Off for the entire organisation.

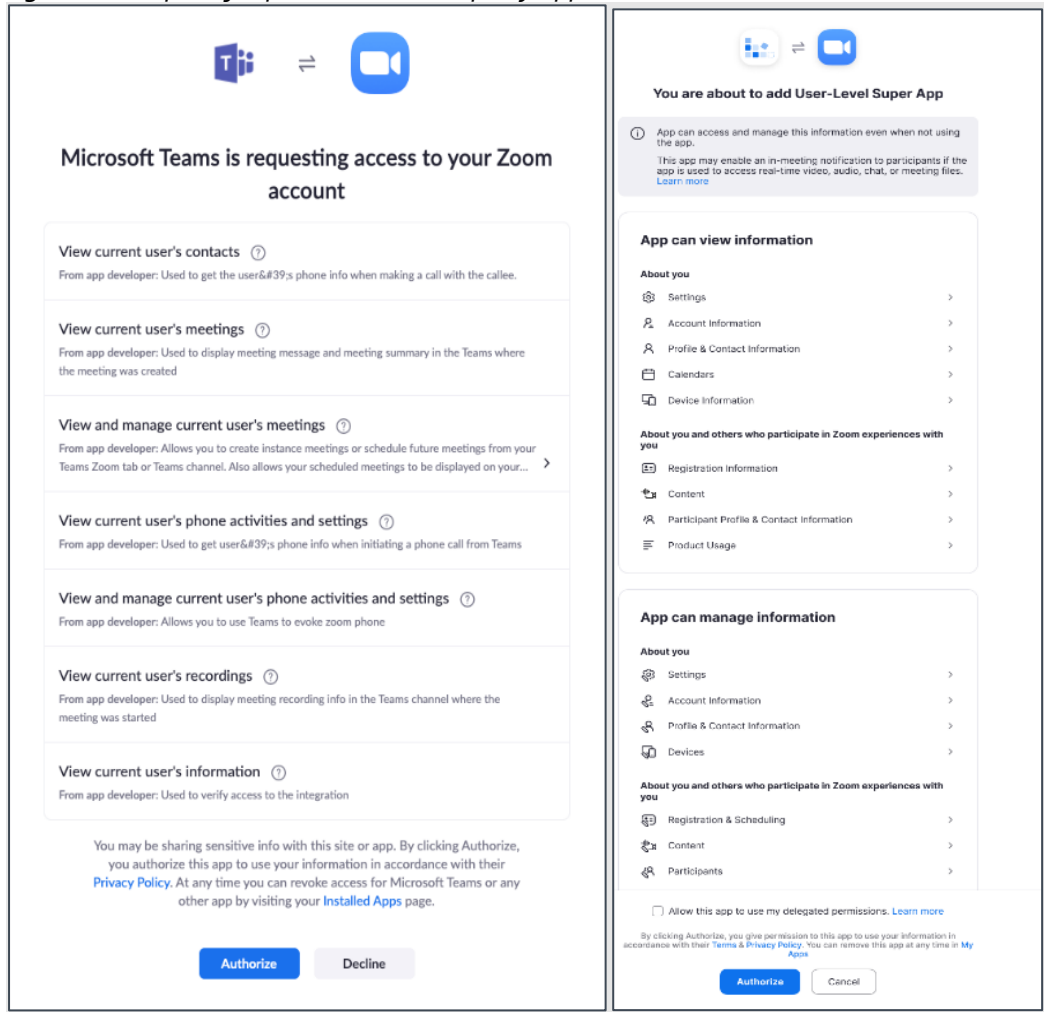
Zoom also gives users a choice if they want to give third parties access to their Zoom Account via the API. See [Figure 28](#) below.

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.

⁸¹ Zoom, Changing settings in the desktop client/mobile app, last updated 26 February 2024, URL: <https://support.zoom.us/hc/en-us/articles/201362623-About-Settings>.

⁸² Zoom, End-to-end (E2EE) encryption for meetings, last updated 28 February 2024, URL: <https://support.zoom.us/hc/en-us/articles/360048660871-End-to-end-E2EE-encryption-for-meetings>.

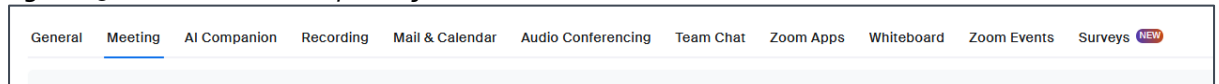
Figure 28: Request for permissions third party app⁸³



4.1.3. Privacy choices and default settings for Hosts

Zoom offers separate data protection controls to users when they act as host. The menu contains 4 main sections, each with many different controls. See [Figure 29](#) below.

Figure 29: Menu with main options for hosts



⁸³ Screenshot made in the browser access to Zoom.

- Access security options via the security icon in the toolbar for quick access to essential in-meeting security controls.
- Add a Feedback tab to the Windows Settings or Mac Preferences
- Use Focus mode, giving participants view of videos without seeing each other⁸⁴
- Allow meeting participants to send a message visible to all participants (default On)
- 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). Hosts can specify allowed file types and maximize file size.
- 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). The host may allow only the host, or all participants, and one participant at a time or multiple participants.

⁸⁴ Zoom, Using focus mode, 29 November 2023, URL: <https://support.zoom.us/hc/en-us/articles/360061113751>.

- 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.
- Require media encryption for 3rd party endpoints: This setting requires third party endpoints for data transfer to use media encryption compliant with Zoom's standards in order to be used during a meeting (default Off).⁸⁵Message deletion: When enabled, participants are allowed to delete their own messages in the meeting chat (default On).
- Enable screenshots: When enabled, participants can send screenshots in chat during the meeting (default On).
- Auto-save: When enabled, chat messages are automatically saved to the host's computer when the meeting ends (default On).
- Allow a co-host: If enabled, a host can add a co-host with the same controls in-meeting.
- Annotation and whiteboard saving: Host may decide to allow participants to save annotated shared screens, and may decide to allow users to share images of shared whiteboards (default On).
- Participant profile photos: Host may hide participant profile photos and only display names of participants (default Off).
- Save Captions: Host may choose which users may save captions or transcripts. Options include, Host, Host and Co-host, anyone who is not an external participant, or participants with specific IP addresses (default On).
- Camera control: Hosts may allow for other users to control the host camera. This option requires both users to have this option enabled, and additionally can be configured so that users in the same Group can take over each other's cameras automatically (default Off).
- AI Companion: Only one feature is currently available in the EU: Smart Recording. This is available to hosts if not disabled by admins. It creates summaries and highlights of the cloud recordings created from Zoom meetings (default Off for hosts).

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)

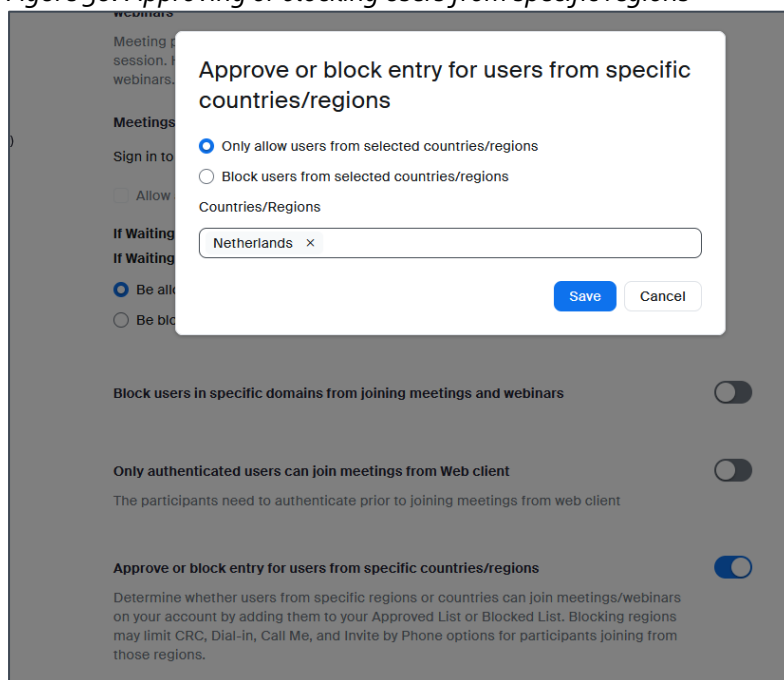
⁸⁵ Zoom. Media encryption for SIP/H.323, Last Updated 30 November 2023, URL: https://support.zoom.com/hc/en/article?id=zm_kb&sysparm_article=KB0065781.

- 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)
- Allow Zoom Rooms to start meeting with Host Key: Allow Zoom Rooms to begin a meeting with a 6-digit code making the user with the code the host (default Off).⁸⁶
- Add watermark: Email addresses embedded into shred content and shared video feeds, or both. Hosts may choose where it is visible and the opacity of the mark.

4.1.4. Allowing or blocking users from specific regions

When users host a meeting, they can allow or block users from selected regions. See [Figure 30](#) below.

Figure 30: Approving or blocking users from specific regions⁸⁷



⁸⁶ Zoom, Claiming host privileges in Zoom Rooms with the host key, Last Updated 11 December 2023, URL: https://support.zoom.com/hc/en/article?id=zm_kb&sysparm_article=KB0069032.

⁸⁷ Zoom, Joining from specific countries/region, 25 March 2024, URL: https://support.zoom.com/hc/en/article?id=zm_kb&sysparm_article=KB0064685.

4.2. 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.

4.3. Privacy controls for admins

Administrators of Zoom Meetings Education 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 an education or research organisation may want to take central technical measures, at the tenant level, 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, 23 different relevant options are discussed, with references to Zoom's documentation how to effectuate the setting.

4.3.1. 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. Thanks to Zoom's participation to the EU US Data Privacy Framework use of E2EE is no longer required to protect the data against the risks of access by government authorities in third countries, but it can still be a very useful measure to protect confidential and sensitive/special categories of personal data. See Section 7 of this DPIA.

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:

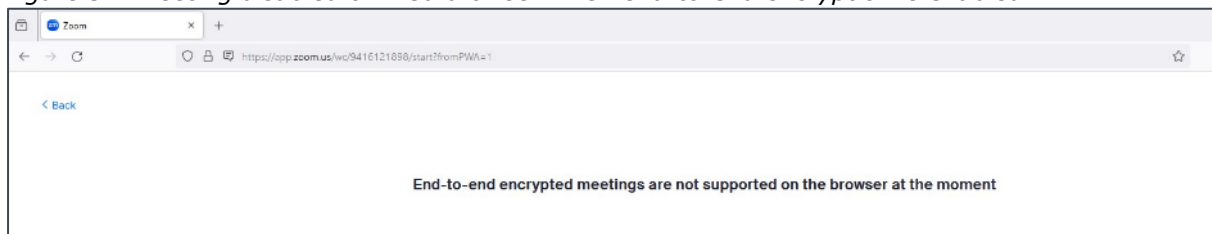
- Join the meeting by telephone
- Join before host
- Cloud recording
- Live streaming

- Live transcription
- Breakout Rooms
- Polling
- Zoom Apps⁸⁸

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.⁸⁹

Enabling end-to-end encryption also disables users from joining Zoom calls through a web browser.

Figure 31: Meeting disabled on web browser when end-to-end encryption is enabled



4.3.2. EU Geolocation

Zoom has completed its EU Cloud offering by the end of 2022. Since, Zoom processes most personal data from EU Education tenants exclusively in Zoom’s EU data centres (in Germany and the Netherlands, see below). This setting applies to all Content Data (such as data exchanged in Meetings, recorded data such as cloud recordings and meeting transcripts, as well as files that are exchanged during a meeting).⁹⁰ See [Figure 32](#) below.

Since the autumn of 2022 Zoom used an EU helpdesk in Romania for its EU customers. In 2023 Zoom has changed to a different subprocessor in Ireland. Zoom ensures that during EU business hours all Support Data are processed in the EU. As shown in [Figure 4](#), Zoom shows customers 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.

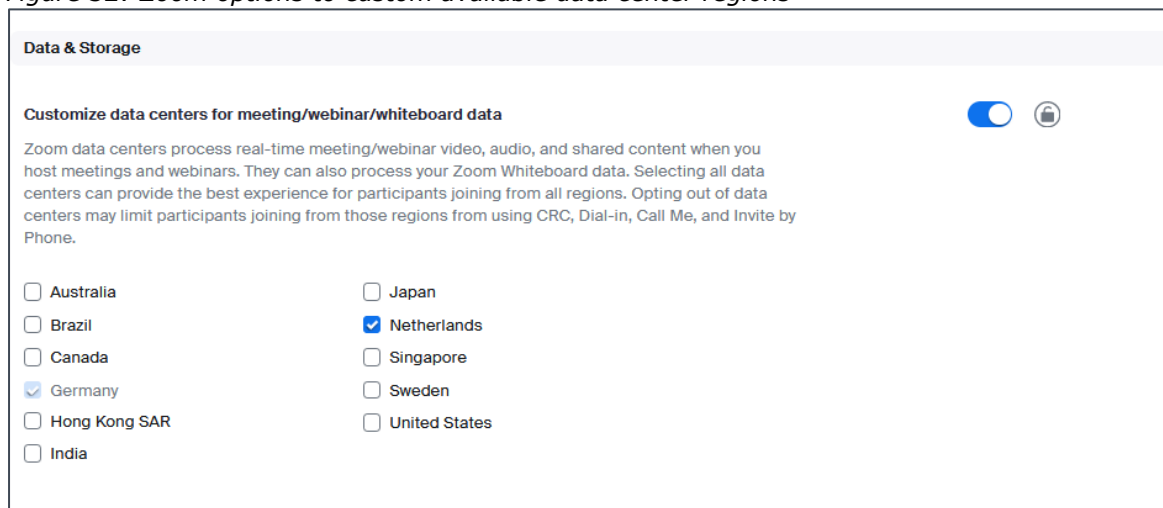
⁸⁸ Zoom, End-to-end (E2EE) encryption for meetings, last updated 28 February 2024, URL: <https://support.zoom.us/hc/en-us/articles/360048660871-End-to-end-E2EE-encryption-for-meetings>.

⁸⁹ Zoom, Enabling and starting local recordings, last updated 20 November 2023, URL: <https://support.zoom.us/hc/en-us/articles/201362473-Enabling-and-starting-local-recordings>.

⁹⁰ Zoom, Selecting data center regions for meetings/webinars, last updated 10 January 2024, URL: https://support.zoom.com/hc/en/article?id=zm_kb&sysparm_article=KB0060026. See also Zoom blog, How Zoom delivers privacy commitments in Europe, 11 July 2023, updated 1 August 2023, URL: <https://blog.zoom.us/zoom-privacy-europe/>.

Zoom also offers options to hosts select the data centers that will be used to process the Content Data when hosting a meeting or webinar.⁹¹ Dutch school and university admins can disable this functionality, and only allow the data to be processed in Germany (home region for all paid EU accounts) and the Netherlands. See [Figure 32](#) below

Figure 32: Zoom options to custom available data center regions⁹²



4.3.3. Public and private in meeting chat

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

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.⁹³

4.3.4. Controls in permanent Team Chat

Admins have privacy related controls for Team Chat, a feature that allows end users to create permanent chat channels in the Zoom client. These controls include:⁹⁴

- Enable end to end chat encryption
- Allow bots to participate in chats and channels
- Enable Personal channel in Chat window
- Allow users to search for each other

⁹¹ Zoom, Selecting data center regions for meetings/webinars, 10 January 2024, URL: https://support.zoom.com/hc/nl/article?id=zm_kb&sysparm_article=KB0060026

⁹² Idem.

⁹³ Zoom, Enabling or disabling in-meeting chat, last updated 14 November 2023, URL: <https://support.zoom.us/hc/en-us/articles/115004809306-Enabling-or-disabling-in-meeting-chat>.

⁹⁴ Zoom, Configuring Zoom Team Chat admin settings, Last Updated 24 November 2023, URL: https://support.zoom.com/hc/en/article?id=zm_kb&sysparm_article=KB0058688

- Allow users to add contacts
- Allow users to chat with others
- Allow users to create channels
- Show users' presence status to external contacts
- Share links to messages and channels in Team Chat
- Schedule a meeting from chat or channel
- The Chat Etiquette Tool allows admins to create policies to prevent unwanted sharing of sensitive information based on defined keywords and text patterns/regular expressions (such as account numbers and social security numbers).
- Allow channel owner and admin(s) to remove messages of other members:

Controls also include those related to retention periods:

- The retention period for messages and files in Zoom's cloud
- The storage of messages on local devices (excluding personal channel messages)
- The storage of edited and deleted message revisions
- The sending of data to a third-party archiving service.

4.3.5. 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."⁹⁵

4.3.6. Use of SSO and Vanity URL

Organisations can deploy SSO for employees to subscribe to Zoom, with an organisational subdomain.⁹⁶ Such a Vanity URL⁹⁷ 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.*"

⁹⁵ Zoom, Advanced chat encryption, last updated 28 October 2023, URL: <https://support.zoom.us/hc/en-us/articles/207599823>.

⁹⁶ Zoom, Quick start guide for SSO, last updated 28 October 2023, URL: <https://support.zoom.us/hc/en-us/articles/201363003-Quick-start-guide-for-SSO>.

⁹⁷ Zoom, Guidelines for Vanity URL requests, last updated 28 October 2023, URL: <https://support.zoom.us/hc/en-us/articles/215062646-Guidelines-for-Vanity-URL-Requests>.

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.”*⁹⁸

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.

4.3.7. 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.⁹⁹

4.3.8. Create a custom privacy disclaimer

Administrators may create a custom (privacy) disclaimer when users join a meeting or sign-in to their account.¹⁰⁰ The disclaimer has variable settings for frequency and whether it may be seen by users internal or external to the organization.

4.3.9. 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.¹⁰¹

⁹⁸ Zoom reply to part A of the DPIA, 19 March 2021, p. 16.

⁹⁹ Zoom, Enabling meeting and webinar auto saving chats, last updated 28 October 2023, URL: <https://support.zoom.us/hc/en-us/articles/360060889932-Enabling-auto-saving-chats>.

¹⁰⁰ Zoom, Creating a Zoom custom disclaimer, 13 December 2021, URL: <https://support.zoom.us/hc/en-us/articles/360051221831>.

¹⁰¹ Zoom, Enabling file transfer in meetings, URL: https://support.zoom.com/hc/en/article?id=zm_kb&sysparm_article=KB0058822.

4.3.10. Do not enable Attendee Feedback

Zoom itself can ask for post-meeting Feedback, through its own surveys. As described in Section 1.7, Zoom has disabled this functionality by default for EU Education customers.¹⁰² Admins can (re-)enable Feedback, but they must be aware that the survey contains an open text field. There is a possibility that end users provide personal data in this text box. That means the organisation shares personal data with Zoom as a data controller.

As shown in [Appendix 1](#) Zoom's own surveys involved the use of a cookie from the US based company Wootric, and hence, traffic with a.o. IP addresses to the USA. Zoom no longer uses Wootric's services. Instead, Zoom uses subprocessor Qualtrix (see [Table 3](#) in Section 6.3).

4.3.11. Do not enable Giphy in Team Chat

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. If the organisation has enabled advanced chat encryption, use of Giphy is technically impossible. To prevent traffic to Giphy as a third party (Zoom does not have a subprocessor agreement with Giphy) admins should not enable this integration in the Team Chat.¹⁰³

4.3.12. Mute individual or all participants upon entry

This meeting setting can help manage participants and prevent distractions and interruptions during a meeting (Zoom-bombing).¹⁰⁴

4.3.13. File transfer

To prevent accidental data breaches, file transfer is disabled by default.¹⁰⁵

¹⁰² Zoom, Managing the end-of-meeting experience feedback survey, last updated 28 October 2023, URL: <https://support.zoom.us/hc/en-us/articles/115005855266-End-of-meeting-experience-feedback-survey>.

¹⁰³ Zoom, Enabling or disabling animated GIF images for Team Chat, last updated 28 October 2023, URL: https://support.zoom.com/hc/en/article?id=zm_kb&sysparm_article=KB0059062.

¹⁰⁴ Zoom, Muting all participants when they join a meeting, last updated 28 October 2023, URL: <https://support.zoom.us/hc/en-us/articles/360060860512-Muting-all-participants-when-they-join-a-meeting>.

¹⁰⁵ Zoom, Sending a file in meetings and webinars, last updated 28 October 2023, URL: <https://support.zoom.us/hc/en-us/articles/209605493-Sending-a-file-in-meetings-and-webinars>.

4.3.14. Annotation

Enabling annotation tools allows meeting participants to collaborate, brainstorm, and draw over shared content. This functionality is disabled by default.¹⁰⁶

4.3.15. 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.¹⁰⁷

4.3.16. Visibility of participants

Admins can allow users to see each other's contact details. The set of controls for contact lists displayed within an organization is described as follows:¹⁰⁸

- List all account users under 'All Contacts': This will allow all users to see all other users under Company Contacts (displayed in the All Contacts section on the Contacts tab). This option does not show contact groups.
- List all Zoom Rooms under 'All Contacts': This will show all Zoom Rooms under Zoom Rooms (displayed in the All Contacts section on the Contacts tab).

Admins can also determine the visibility of contact groups:

- Visible to anyone, searchable by anyone: All users can see the group in the client and app (displayed in the All Contacts section on the Contacts tab). All users can search for group members.
- Visible to members only, searchable by anyone: Only members can see the group in the client and app (displayed in the All Contacts section on the Contacts tab). All users can search for group members.

¹⁰⁶ Zoom, Enabling or disabling annotation tools for meetings, last updated 23 November 2023, URL: <https://support.zoom.us/hc/en-us/articles/4409894568845-Enabling-or-disabling-annotation-tools-for-meetings>.

¹⁰⁷ Zoom, Adjusting your video layout during a virtual meeting, last updated 9 November 2023, URL: https://support.zoom.com/hc/en/article?id=zm_kb&sysparm_article=KB0063672.

¹⁰⁸ Zoom, Managing user groups and settings, Last Updated 28 October 2023, URL: https://support.zoom.com/hc/en/article?id=zm_kb&sysparm_article=KB0062584#h_01G371HC1ZPB3RR4P098X60NCN



- Visible to members only, searchable by members only: Only members can see the group in the client and app (displayed in the All Contacts section on the Contacts tab). Group members are only searchable by other group members.

4.3.17. 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.¹⁰⁹

4.3.18. Polling

With the control for polling, the admin can add 'Polls' to the meeting controls. This allows hosts to survey the attendees through polls.¹¹⁰ EU Education customers can integrate survey services from their own subprocessors in Zoom.

4.3.19. 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 33 below).

4.3.20. 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.

¹⁰⁹ Zoom, Host and co-host controls in a meeting, last updated 9 November 2023, URL: <https://support.zoom.us/hc/en-us/articles/201362603>.

¹¹⁰ Zoom, Enabling polling for meetings, last updated 28 November 2023, URL: <https://support.zoom.us/hc/en-us/articles/4412324684685>.

Figure 33: Zoom explanation about account permissions for apps¹¹¹

Change Account Permissions

1. Click **Manage**.
2. Under **My Admin Dashboard**, click **Permissions** to change your pre-approval settings.

Note: Pre-approval will be required by default when you create an account. If you do not want apps to be pre-approved before they can be installed by members, you can change your permissions after your account is made.
3. As an Admin, you can restrict the members on your account to only install apps that are pre-approved. Enable or disable the setting **Require all the apps that are listed on the Zoom App Marketplace to be pre-approved**.
4. You can choose to exclude types of published apps from this requirement:
 - **Exclude apps created by Zoom:** Allows your members to install any app created by Zoom without first requiring pre-approval. These apps will have "By Zoom" listed under their name.
 - **Exclude apps created by my account members:** Allows your members to install any app created by users on your account without first requiring pre-approval.
5. You can choose to exclude types of unpublished apps from this requirement:
 - **Exclude apps created by Zoom:** Allows your members to install any unpublished app created by Zoom without first requiring pre-approval.
 - **Exclude apps created by my account members:** Allows your members to install any unpublished app created by users on your account without first requiring pre-approval.

Permissions

Requiring pre-approval restricts users on your account from installing any kinds of apps that are not pre-approved. When enabled, your users will not be able to install apps that are not pre-approved. Changing this setting does not affect existing subscriptions.

Require all the apps that are listed on Zoom App Marketplace to be pre-approved 🔵

Your account users will only be able to install a Marketplace listed app after your pre-approval.

Exclude apps created by Zoom

Exclude apps created by my account members

Require all the apps that are not currently listed on Zoom App Marketplace to be pre-approved 🔵

Your account users will only be able to install a private app or a Marketplace listed app using its development credential after your pre-approval.

Exclude apps created by Zoom

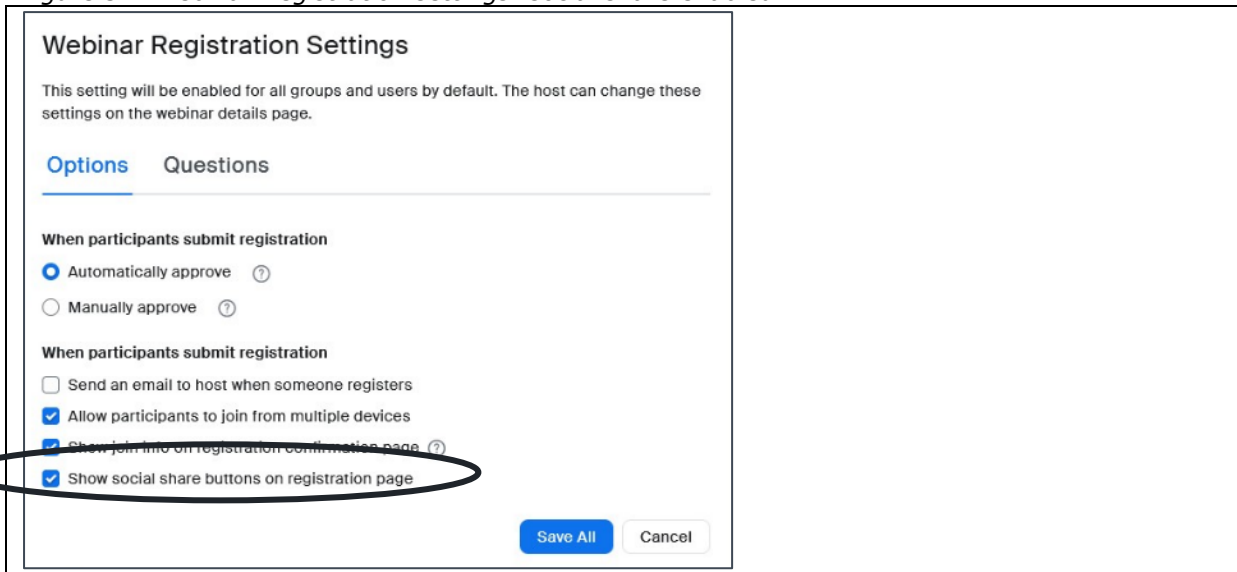
Exclude apps created by my account members

4.3.21. Webinar settings: social share, tracking pixels and livestreams

Owners and administrators have the ability to disable third party social share buttons on the registration pages for Zoom webinars. The social share buttons are **on** by default. This enables end users to share the webinar announcement on social media. If the webinar is not open to a general public, administrators should disable these social share buttons.

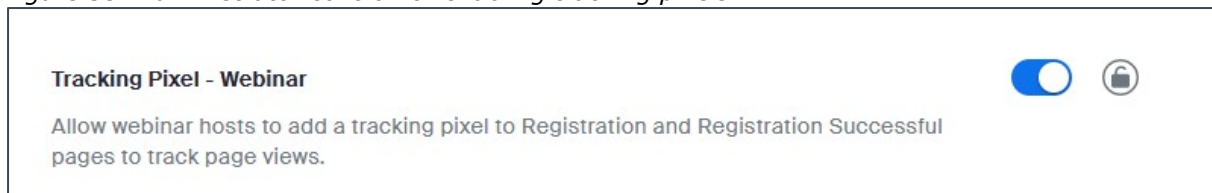
¹¹¹ See also Zoom, Admin management of the Zoom App Marketplace, last updated 4 January 2024, URL: <https://support.zoom.us/hc/en-us/articles/360032447812-Managing-Zoom-Marketplace>.

Figure 34: Webinar Registration settings: social share enabled



Owners and administrators also have the ability to place tracking pixels on the invitation and confirmation pages of Zoom webinars if they use Zoom’s sub processor Twilio to send these mails.¹¹² These pixels track traffic and engagement from users who reach the page from the emails that invite them to join a webinar. Zoom provides users with a tutorial for setting up a Facebook tracking pixel.¹¹³ The ability to set tracking pixels by a webinar host is on by default. If the organisation does not obtain prior consent from recipients, they should disable this feature.

Figure 35: Administrator control for enabling tracking pixels



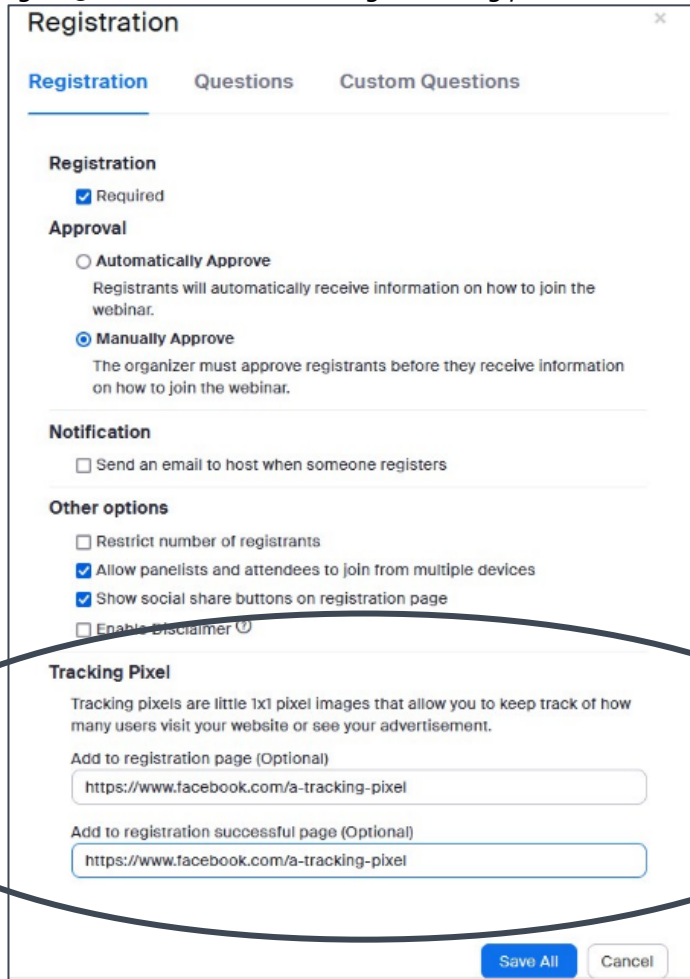
As shown in [Figure 36](#) and [Figure 37](#) below, Privacy Company used the fictional URL www.facebook.com/a-tracking-pixel to represent a tracking pixel.

However, EU Education customers do not have to use Twilio: they can also integrate their own subprocessors for mailing services and invitation management in Zoom.

¹¹² Zoom, Enabling - webinar tracking pixel, last updated 28 October 2023, URL: https://support.zoom.com/hc/en/article?id=zm_kb&sysparm_article=KB0066874.

¹¹³ Zoom, Using Facebook Pixel with Zoom, last updated 28 October 2023, URL: https://support.zoom.com/hc/en/article?id=zm_kb&sysparm_article=KB0066596

Figure 36: Webinar host enabling a tracking pixel



The screenshot shows a 'Registration' settings window with the following sections:

- Registration**
 - Required
- Approval**
 - Automatically Approve
Registrants will automatically receive information on how to join the webinar.
 - Manually Approve
The organizer must approve registrants before they receive information on how to join the webinar.
- Notification**
 - Send an email to host when someone registers
- Other options**
 - Restrict number of registrants
 - Allow panelists and attendees to join from multiple devices
 - Show social share buttons on registration page
 - Enable disclaimer ⓘ
- Tracking Pixel**

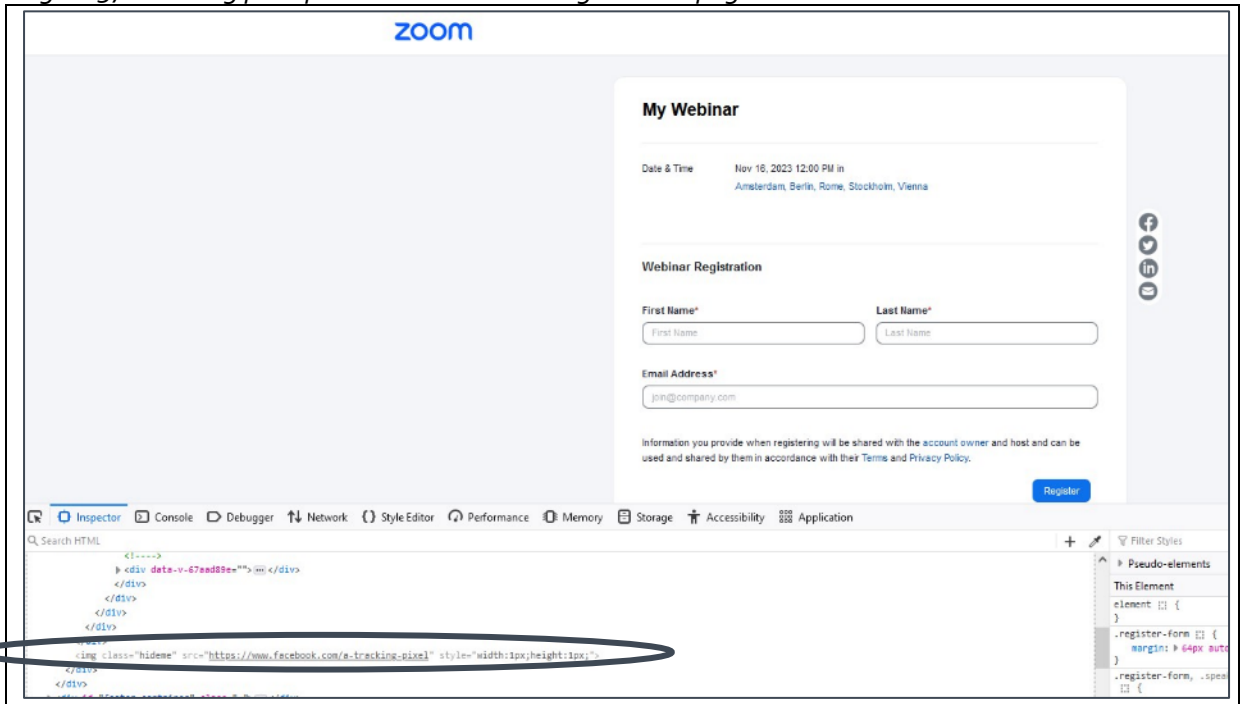
Tracking pixels are little 1x1 pixel images that allow you to keep track of how many users visit your website or see your advertisement.

Add to registration page (Optional)

Add to registration successful page (Optional)

Buttons: Save All, Cancel

Figure 37: Tracking pixel present on a webinar registration page



Users are not explicitly informed of the presence of a tracking pixel on a webinar registration or confirmation page. Zoom presents the users with a message that states:

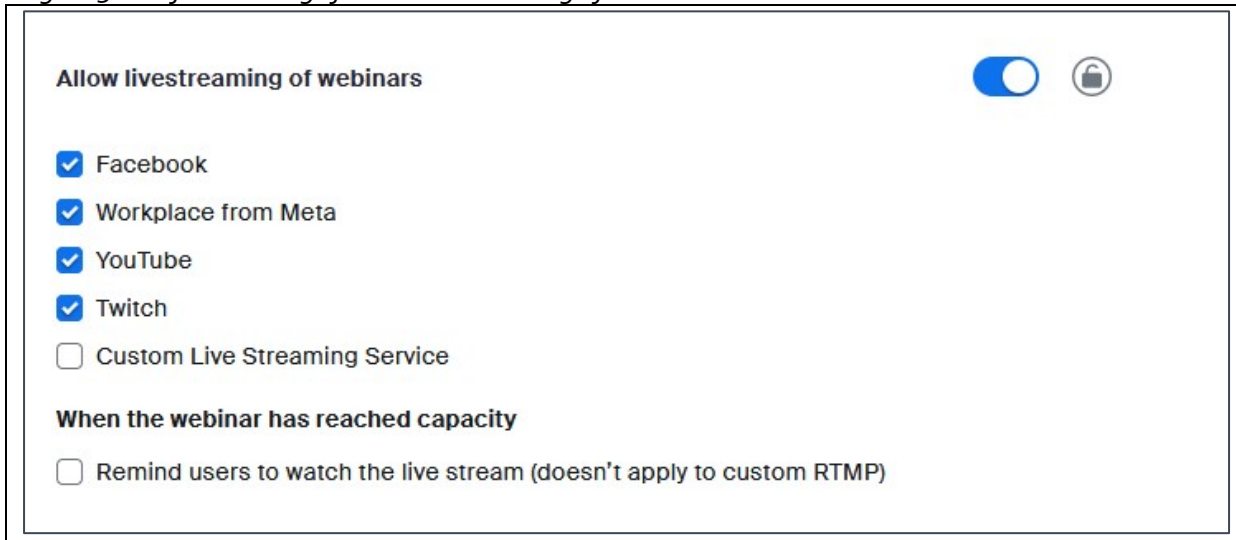
“Information you provide when registering will be shared with the account owner and host and can be used and shared by them in accordance with their Terms and Privacy Policy.”

This message contains links to the account owners terms of service, privacy policy, and to Zoom’s “Understanding Zoom privacy alerts” article.¹¹⁴

Owner and administrator accounts have the ability to allow or disallow the livestreaming of webinars, and the specific third party livestreaming services used to do so. Livestreaming is enabled by default and the services Facebook, Workplace from Meta, Youtube, and Twitch are enabled. To prevent unauthorised processing by these social media for their own commercial purposes, owners and administrators are advised to disable these third party services.

¹¹⁴ Zoom, Understanding Zoom privacy alerts, last updated 4 November 2023, URL: https://support.zoom.com/hc/en/article?id=zm_kb&sysparm_article=KB0059866.

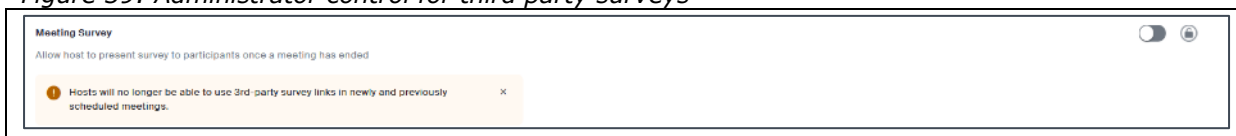
Figure 38: Default settings for the livestreaming of webinars



4.3.22. Third Party Surveys

Owners and administrators have the ability to allow users who create meetings to share surveys with meeting participants.¹¹⁵ These surveys may be from a third party, such as Google or Survey Monkey. This option is (also) disabled by default. To prevent data leakage to third parties that may process these data for their own commercial purposes, admins should not enable this option. Zoom has confirmed that universities can integrate with their own survey / mailing tool.

Figure 39: Administrator control for third party surveys



4.3.23. Zoom AI Companion

Even though Zoom AI Companion was out of scope of the DPIA, and the data processing could not be tested, organisations will have to make a choice about its use. Zoom offers seven features through the integration of AI tools with its services.¹¹⁶ Include in this list is a feature that has been available prior to the release of AI Companion: Smart Recording. This is the only AI feature currently available for administrators with an EU Education license. Among other things, this feature divides

¹¹⁵ Zoom, Enabling meeting surveys, last updated 12 January 2024, URL:

https://support.zoom.com/hc/en/article?id=zm_kb&sysparm_article=KB0067657.

¹¹⁶ Zoom, Settings and Configuration for Zoom AI Companion, last viewed 16 November 2023, URL:

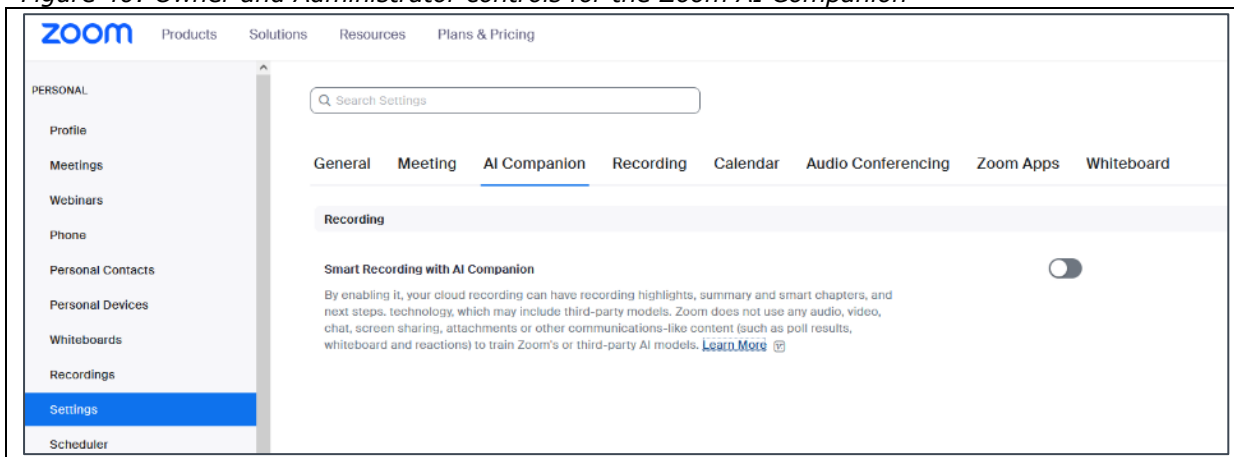
https://support.zoom.com/hc/en/category?id=kb_category&kb_category=891c5079c3bdf1104b490e8dc00131da.

users' cloud recordings of meetings into chapters and provides and highlights of portions of the meeting.¹¹⁷

Smart Recording is disabled by default. The switch to enable the feature is available to owner and admin accounts in the AI Companion section of the settings menu, as shown in [Figure 40](#) below.¹¹⁸

Zoom processes the data for the AI Companion within the specific environment of the customer. As discussed in Section 2.1 Zoom does not use these data for any training/learning or other improvement of its own, or its third parties' artificial intelligence models.¹¹⁹

Figure 40: Owner and Administrator controls for the Zoom AI Companion



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.¹²⁰ 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

¹¹⁷ Zoom, Using Smart Recording with AI Companion, last updated 28 October 2023, URL: https://support.zoom.com/hc/en/article?id=zm_kb&sysparm_article=KB0061101.

¹¹⁸ Zoom, Enabling Smart Recording with AI Companion, last updated 27 October 2023, URL: https://support.zoom.com/hc/en/article?id=zm_kb&sysparm_article=KB0058511.

¹¹⁹ Zoom blog, How Zoom's terms of service and practices apply to AI features, 7 August 2023, updated 7 February 2024, URL: <https://blog.zoom.us/zooms-term-service-ai/>.

¹²⁰ Article 5(1)(b) GDPR.

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 for the public website). The agreed limited purposes are described in Section 5.2 below.

5.1. Purposes education and research organisations

The general interests education or research 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, education and research 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 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:

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.¹²¹

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

Providing the service

In reply to this Update DPIA, Zoom has explained that as part of providing the service it necessarily has to route all log-in attempts via its central servers in the USA. Zoom processes a hashed version of the e-mail address (or tokenised user ID if an organisation uses SSO for login) and the unique User ID to recognise who the user is, and based on that identity, to reroute users to their chosen geolocation (for Dutch Education customers: the EU geolocation). If Zoom would not have such a central routing system, each log-in request would have to be shared with all global geolocations to find out to what geolocation that user belongs to. That would increase the amount of international data transfers and would create latency. Zoom's explanations are plausible that this data processing is necessary to operate Zoom.

Zoom has also explained it sends service notifications to users when such communications are strictly necessary to be able to provide the service. Such notifications are mails in reply to use of the "Forgot My Password" option, "User has joined your meeting", and DSAR notifications. Users cannot opt-out of this processing. Zoom uses a USA based subprocessor for these notifications, Twilio. Zoom has ensured SURF that it has disabled the tracking pixel in the mails to EU Education customers.¹²²

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.*"¹²³ In reply to this DPIA, Zoom explained

¹²¹ Zoom DPA, Clause 2.2

¹²² Zoom mail in reply to this update DPIA, 8 March 2024.

¹²³ Zoom DPA, Annex II, 18 Vulnerability Monitoring

that it uses third party tools for this purpose¹²⁴ but Zoom has confirmed that the third party malware detection vendors do not have access to any personal data from customers.¹²⁵

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.”*¹²⁶

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.

Zoom explained in the context of this DPIA it uses a third-party vendor to perform annual penetration tests of the production networks.¹²⁷ 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.”*¹²⁸ That is why such vendors are not separately mentioned in the list of subprocessors for the EU Education 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.”*¹²⁹ 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

¹²⁴ Zoom reply to part A of the DPIA, 19 March 2021, p. 53.

¹²⁵ Zoom response to this Update DPIA, 8 March 2024.

¹²⁶ Zoom DPA, Annex II, 18 *Vulnerability Monitoring*.

¹²⁷ Zoom Answer to DPIA questions, 23 November 2020, answers to Q4f.

¹²⁸ Zoom reply to part A of the DPIA, 19 March 2021, p. 53.

¹²⁹ Zoom reply to part A of the DPIA, separate spreadsheet, 19 March 2021.



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:

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).¹³⁰

These purposes are limitative. They have all been minutely discussed and defined in dialogue with Zoom. The scope of the processing for these purposes 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.”¹³¹

The first purpose authorises Zoom to send commercial messages to its commercial contacts, but conversely, prohibits the sending of commercial mails to admins and end users. Zoom may only send

¹³⁰ Zoom new DPA, Section 2.4.

¹³¹ Zoom Answers to DPIA questions, answer to Q4i.

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 [of non-commercial communication], but I could imagine it might be relevant if we needed to meet a legal obligation, such as a data breach requirement.”*¹³²

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. Initially, this DPIA included a lengthy table 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 to US government authorities. There was also a separate Data Transfer Impact Assessment (DTIA).

This DTIA is no longer necessary. Since 2022 Zoom processes most of the personal data from its EU Education customers in the EU, and only incidentally transfers data to third countries, if the customer consents to the transfer (for support outside of office hours from the Philippines, or if an end user participates in a meeting organised by an organisation outside of the EU, or travels to a third country and uses the Zoom service).

The only ongoing systematic transfer of data outside of the EU after the end of 2022 is the transfer of pseudonymised user account data to the USA to allow users to log into their account, and the collection of clipped IP addresses of end users in the USA for tax compliance reasons (data with reduced identifiability). Once the user is identified, personal data are exclusively processed in the EU. Additionally, Zoom systematically transfers aggregated non-personal Diagnostic Data to Zoom in the USA. Incidentally, some personal data may be transferred to the Trust & Safety team in the USA, for example in case of a complaint, or transferred to a third country in case Zoom were to receive an order for compelled disclosure from a government authority.

Based on the July 2023 adequacy decision from the European Commission for participants to the Data Privacy Framework agreement in the USA, there is no need any more for data controllers in the EU to perform a DTIA for transfers to the USA. SURF continues to rely on SCCs instead of the Data Privacy Framework. This mechanism, and the factual data transfers are discussed in Section 8. However, two US legal obligations are still relevant to mention: a data retention obligation, and the requirement to combat the distribution of child sexual abuse material.

A relevant legal obligation not explicitly discussed by the European Commission 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

¹³² Idem, p. 22.

evidence of foreign derived income by retaining the IP addresses of the end users in the EU for a period of 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 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.”¹³³

Zoom has decided to retain clipped IP addresses for 10 years from the date of collection.

Another specific US legal obligation is the requirement for US communication providers to detect and report Child Sexual Abuse Material (CSAM). This scanning is separately defined in the DPA. It involves the use by Zoom in the EU 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.¹³⁴

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>.”¹³⁵* 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.

¹³³ 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>.

¹³⁴ URL: <https://www.missingkids.org/footer/about>.

¹³⁵ Zoom Answers to DPIA questions, 23 November 2020, Answer to Q4d.

Zoom has assured that Microsoft's PhotoDNA only reports 'hits' to the Trust & Safety Team in the USA 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 within an image. It can only be used to identify copies of known CSAM, for which NCMEC has assigned a PhotoDNA signature."*¹³⁶

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."*¹³⁷

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*

¹³⁶ Zoom reply to part A of the DPIA, 19 March 2021, p. 54.

¹³⁷ Zoom DPA, Clause 2.10.

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.”¹³⁸

Improving and optimizing

In reply to questions from SURF about the fourth purpose, with the very broad terms ‘*improving and optimizing*’ Zoom explained that optimization of the services means use of the data for technical improvement: “*to help the services run most efficiently, for example, balancing network load.*”¹³⁹

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.

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.*”¹⁴⁰

The example revealed that Zoom permitted itself to perform analyses of uptake or usage at an individual Education 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 education and research organisations need to have a legal ground.

SURF, Privacy Company and Zoom have discussed different aggregation models in 2023 to prevent export of identifiable data to Zoom’s HQ. Zoom has chosen the most restrictive model, whereby it aggregates all EU data in the EU, before transferring the statistics about daily and monthly active users to the USA. This privacy friendly aggregation comes at a cost for Zoom: it prevents Zoom from

¹³⁸ E-mail Zoom to SURF, 3 February 2022.

¹³⁹ Ibid. Zoom Answers to DPIA questions, answer to Q4i.

¹⁴⁰ Zoom reply to part A of the DPIA, 19 March 2021, p. 57.

deduplicating EU users when they travel outside of the EU. Anonymisation and the application of privacy by design are discussed in Sections 9.2 and 9.3 of this report.

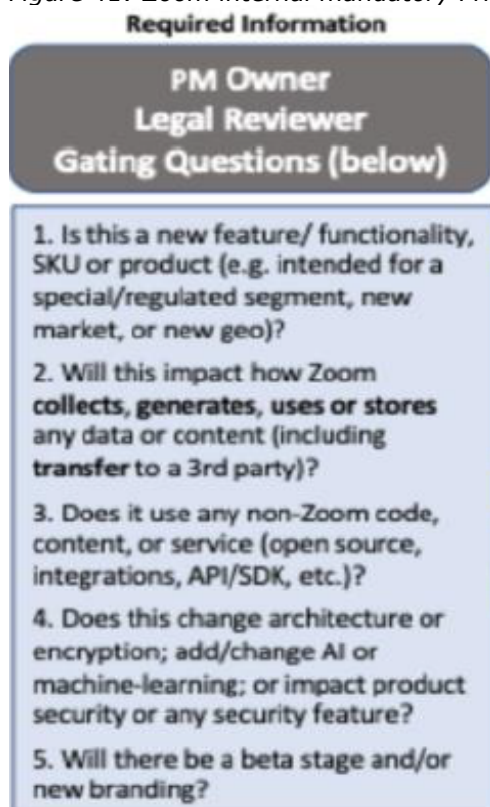
Feedback

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 may 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 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.

Figure 41: Zoom internal mandatory Privacy by Design questions



Required Information

**PM Owner
Legal Reviewer
Gating Questions (below)**

1. Is this a new feature/ functionality, SKU or product (e.g. intended for a special/regulated segment, new market, or new geo)?
2. Will this impact how Zoom **collects, generates, uses or stores** any data or content (including **transfer to a 3rd party**)?
3. Does it use any non-Zoom code, content, or service (open source, integrations, API/SDK, etc.)?
4. Does this change architecture or encryption; add/change AI or machine-learning; or impact product security or any security feature?
5. Will there be a beta stage and/or new branding?

6. Processor or (joint) controller

This section assesses the data protection role of Zoom and its customers (the education and research organisations) in the context of the Zoom Meetings Education 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 2022 DPA between SURF and Zoom, 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.

The 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."*¹⁴¹

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 2022 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 the education and research organisations to verify their compliance with the obligation as data controllers to only process personal data for specific and explicit purposes.

The 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 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, it

¹⁴¹ Zoom DPA, Clause 2.1.

must 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 published a useful explanation of how data controllers can allow data processors to process personal data for these necessary operations.¹⁴²

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 by Privacy Company]:

“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.”¹⁴³

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 the DPA. Legally and factually Zoom qualifies as a data processor.

6.3. Subprocessors

Through the 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.¹⁴⁴

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*

¹⁴² 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>.

¹⁴³ Idem.

¹⁴⁴ Zoom, Third-Party Subprocessors, effective 3 November 2023, URL: <https://zoom.us/subprocessors>. SURF agreed to the list published on 30 December 2021.

terms of this Agreement and this Addendum. Authorized Subprocessors may include Zoom Affiliates but shall exclude Zoom employees, contractors and consultants.”¹⁴⁵

Zoom’s guarantee of EU-only processing is leading. All other subprocessors that process data outside of the EU can only process personal data from Dutch Education customers in two circumstances: if customers explicitly consent to the use of these services (opt-in), or if an end user travels outside of the EU and connects to a Zoom meeting. The subprocessors that EU customers will inevitably use are marked green in Table 3 below. This includes the support services. Though use is not mandatory, the processing is not purely incidental.

Zoom’s current list of subprocessors also includes OpenAI and Anthropic as subprocessors in the USA. ¹⁴⁶Zoom has SCCs with those parties, but since the algorithmic models and Large Language Models are not (yet) available for EU Education customers, these subprocessors are not in scope of this Update DPIA.

Subprocessors marked with an *Asterix (Microsoft Switzerland and Oracle Mexico and Switzerland) do not process personal data of Dutch Education customers. Data processing by some subprocessors is optional, in that case the word ‘MAY’ is spelled in capitals and emphasised.

Table 3: Zoom list of authorised subprocessors for EU Education customers¹⁴⁷

Subprocessor	Purpose	Category of personal data	Location	Type of agreement
Amazon Web Services	Cloud Service Provider	<ul style="list-style-type: none"> 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 	E.U.	SCCs
Apple	Push notifications on iOS phones. Customers can choose not to use this service.	Apple MAY process <ul style="list-style-type: none"> Chat Message Notification SMS Message Notification PBX (Phone Call) Message Notification 	United States	SCCs
Cloudflare	Security/CDN	IP address	E.U.	SCCs

¹⁴⁵ Zoom DPA, Clause 1.2.

¹⁴⁶ Zoom Third-Party Subprocessors & Zoom Affiliates, URL: <https://explore.zoom.us/en/subprocessors/>

¹⁴⁷ Attached as Annex III to the DPA that is part of the contract with SURF for the Dutch universities.

Google Cloud Platform	Cloud service provider	Real time meeting and webinar traffic (only if end user is in Taiwan or China)	Taiwan	SCC
Google Firebase	Push notifications on Android phones. Customers can choose not to use this service.	Google MAY process <ul style="list-style-type: none"> • Chat Message Notification • SMS Message Notification • PBX (Phone Call) Message Notification 	United States	SCCs
MaestroQA	Support Quality Assurance	Support related Communications Content such as cloud recordings or in-meeting chat transcripts MAY be shared with MaestroQA but only if Customer chooses to provide it directly to a Zoom support agent through a support interaction, i.e., as an attachment to a support ticket.	Ireland	SCCs
*Microsoft	Cloud Service Provider.	<ul style="list-style-type: none"> • 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 	Switzerland ¹⁴⁸	SCCs
One Trust	Cookie Consent Management and Data Subject Access Request Platform	For the Cookie Consent Management: <ul style="list-style-type: none"> • User cookie preference • IP address • Location (derived from IP address) 	United States	SCCs

¹⁴⁸ EU customers can select Switzerland as the storage location for their content instead of Germany. See the Zoom support page, Managing Communications Content storage location, URL: https://support.zoom.com/hc/en/article?id=zm_kb&sysparm_article=KB0066473.



		<p>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:</p> <ul style="list-style-type: none"> • Name • Email address • Plan type • User role • Country/state of residence 		
*Oracle	Cloud Service Provider	<ul style="list-style-type: none"> • Real-time meeting and webinar traffic • Meeting and call recordings • Transcriptions of meeting or call recordings 	Mexico, United States	Binding Corporate Rules (BCRs) + new SCCs in progress
Qualtrics	Feedback, Reviews, and Survey Responses	<p>If a customer chooses to provide feedback, reviews, or survey responses to Zoom, then Qualtrics MAY process:</p> <ul style="list-style-type: none"> • Email address • IP address • Account information • Customer Content or any data the customer chooses to provide in the feedback, survey, or review 	Germany	SCCs
SendSafely	Encrypted file transfer service	Communications Content such as attachments MAY be shared with SendSafely but only if Customer chooses to provide it directly to a Zoom support agent through a support interaction (i.e., as an attachment to a support ticket).	United States	SCCs
ServiceNow	Cloud-based Customer Service Platform	Communications Content such as cloud recordings or in-meeting chat transcripts MAY be shared with ServiceNow but only if Customer chooses to provide it directly to a Zoom support agent through a support interaction.	Germany	SCCs
TaskUS	Support Providers	Communications Content such as cloud recordings or in-meeting chat transcripts	Philippines	SCCs

		MAY be shared with TaskUS but only if an EU Customer chooses to provide it directly to a Zoom support agent in the Philippines through a support interaction.		
Twilio	Service notifications from Zoom	For example in case of a password reset	United States	SCCs
	[optional] customer e-mail invitations and notifications emails to webinar registrants with Webinar details.	Customers MAY share <ul style="list-style-type: none"> • Name • Email address • Meeting or webinar subject • Meeting/webinar ID • Meeting date and start time • Tracking pixel (can be disabled) 		
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 an EU Customer chooses to provide it directly to a Zoom support agent in the USA through a support interaction.	United States	BCRs + onward transfers in the EU US DPF and new SCCs in progress
		Otherwise tickets are processed by the German subprocessor ServiceNow.		

Zoom’s affiliates (not subprocessors) 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 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.”¹⁴⁹

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.¹⁵⁰

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.”¹⁵¹*

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 EU data centres.

Zoom uses two EU-based subprocessors for its Support Services: ServiceNow in Germany as platform for the tickets and MaestroQA in Ireland as helpdesk. Additionally, Zoom operates two other helpdesks outside of the EU, one in the USA and the Philippines (TaskUS).

Mid 2022 Zoom complied with its commitment to offer EU-exclusive support. At the time, Zoom worked with different subprocessors for its EU customers: a subprocessor in Romania provided the support, and used a separate EU Zendesk instance as platform. Currently Zoom works with the Irish

¹⁴⁹ Zoom new DPA, Clause 7.2.

¹⁵⁰ Idem, Clause 5.4.

¹⁵¹ Idem, Clause 5.6.

subprocessor MaestroQA for support, and the tickets are registered in a separate EU instance of the German subprocessor Service Now.

Only if admins urgently need support outside of regular EU working hours, they can consent to the use of TaskUS as a subprocessor in the Philippines, or the use of ServiceNow as subprocessor in the USA, 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 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 the additional risks of the use of such tools, but only mentions the technical use of a tracking pixel in such mails.

6.4. 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 further process some (limited) personal data for its own business purposes, when the processing is necessary for these legitimate purposes. 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 and SURF also agreed that Zoom is allowed to produce statistics on the number of procured licenses, compared with the amount of used licenses per tenant, as part of regular customer relationship management.

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 (tenant) level) for the last three purposes is equally necessary for Zoom's legitimate financial and technical business operations. The agreed procedures to comply with legal obligations (second purpose), is discussed separately below, in Section 6.4.1.

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 French supervisory authority CNIL describes a solution to this dilemma: controllers may authorise their processors to 'further' process some personal data on their own behalf.¹⁵² 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 being qualified as factual 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.

¹⁵² 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>.

6.4.1. 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.¹⁵³ 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 without being able to redirect that order to the customer/controller. Such a disclosure 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 notify Customer and provide a copy of the demand unless legally prohibited from doing so. For example, through a so-called gagging order.”*¹⁵⁴

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.

¹⁵³ 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.”*

¹⁵⁴ Zoom DPA, Clause 9.2.

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.¹⁵⁵

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.

Twice per year, Zoom publishes a transparency report about mandatory disclosures to government authorities. On 18 December 2020, Zoom published its first semi-annual Transparency report.¹⁵⁶ The reports distinguish between disclosure to US authorities, and to other international requests. Zoom explains its policy: *“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.”*¹⁵⁷

Zoom has published a blog about these commitments.¹⁵⁸ As shown in [Figure 42](#) below, Zoom publicly commits to challenge all government requests by default, when possible.

Figure 42: Zoom blog about compelled disclosure to government authorities

Data protection by default

We do not provide user information to any government unless required to by law or in bona fide emergencies. Any request for user information must come through our single point of intake. ***There are no exceptions.***

We will challenge all government requests for public sector or enterprise customer data where there is a lawful basis for doing so.

¹⁵⁵ Zoom new DPA, Clause 9.2.

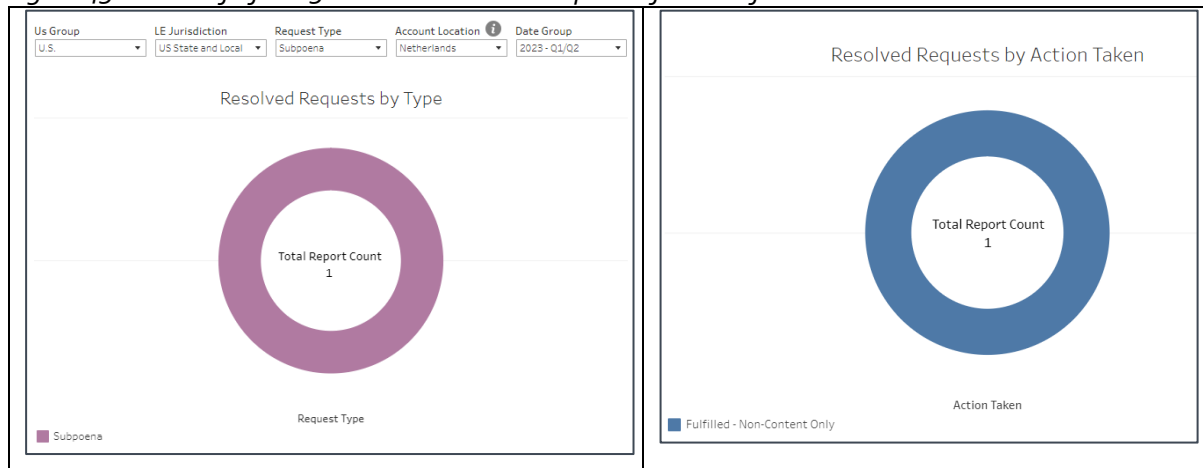
¹⁵⁶ Zoom first transparency report, URL: <https://explore.zoom.us/docs/en-us/trust/transparency-12-18-2020.html>.

¹⁵⁷ Zoom, Transparency Report, 02. U.S. Requests, bottom of the page, URL: <https://explore.zoom.us/en/trust/transparency/>.

¹⁵⁸ Zoom, Government Requests and Data Protection, 18 January 2022, URL: <https://blog.zoom.us/government-requests-and-data-protection/>.

Zoom also explains in this 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.”*¹⁵⁹

Figure 43: First half of 2023: Zoom received 1 subpoena for data from a customer in NL



In Zoom’s most recent transparency report, covering the period from 1 January to 1 July 2023, Zoom discloses that it has received 1 US subpoena for data for a person in the Netherlands, but did not provide the information, because the person did not have a Zoom account. See [Figure 43](#) above.

It follows from the pull-down menu that Zoom did not receive any law enforcement requests for personal data in the Netherlands from Dutch or any international authorities.

In previous transparency reports (starting in January 2021), Zoom did not specify the account location, or the type of license (consumer, Business, Enterprise or Education). In the most recent report, Zoom has increased the transparency, and discloses that it has received a total of 926 requests from US authorities relating to all of its global customers, and replied to 5 requests for data from Education licenses. It is unlikely that these 5 requests involve data from Dutch Education customers, as Zoom has previously specified in the DTIA from February 2022 that it had never disclosed any personal data from EU public sector customers to any US government authority, including secret services.

In almost 80% of the 926 requests, Zoom ‘fulfilled’ the request by answering ‘null’. This only reflects that prior to January 2023, Zoom did not collect these specific statistics, and hence, cannot provide separate answers in previous transparency reports. To prevent misunderstandings, Zoom

¹⁵⁹ Idem.

recommends using the date group filter to only view the Q1 and Q2 data of 2023 for a separate statistic on account data.

7. Interests in the data processing

This section outlines the different interests of Zoom and the Dutch education and research organisations in the use of Zoom Meetings. The interests of the education and research 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 education and research organisations is analysed in part B of this DPIA.

7.1. Interests education and research organisations

Dutch education and research organisations have security, efficiency and compliance reasons to use (paid) videoconferencing services such as Zoom Meetings Education.

A key data protection and security benefit of the use of the Education 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 the newly developed take-out for admin behaviour, is essential for education and research organisations to comply with their own obligations as data controllers to detect security incidents and data breaches.

With Zoom Meetings Education, 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 education and research organisations do not sign-up for an Education 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 education and research 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. Zoom has also completed its EU Data Boundary. Though there are no longer any high risks if organisations transfer data to participants to the Data Privacy Framework in the USA (since the new adequacy decision from the European Commission from 10 July 2023), the processing in the EU prevents risks related to transfers to third (non-adequate) countries.

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.

7.2. Interests of Zoom

Zoom has a strong financial and economic interest in upselling customers of its free Basic services to a paid subscription service in order to generate revenue, and to increase the size of existing subscriptions.

Zoom is a publicly held company since 18 April 2019 and publishes annual financial reports as Form 10-K for the fiscal years 2020-2022 ending 31 January.¹⁶⁰ In these forms Zoom describes that its user base skyrocketed during the global outbreak of the COVID-19 pandemic. Zoom went from 10 million users at the end of 2019, to 300 million in April 2020.¹⁶¹

Since, Zoom is focussing on expanding its market share in paid customers. Zoom writes: “*As of January 31, 2023, 2022, and 2021, we had approximately 213,000, 191,000, and 141,100 Enterprise customers, respectively.*” The revenue from Enterprise (and Education) customers also increased to 54.8% of total revenue in 2022, compared to 47.6% and 45.6% in 2021 and 2020.¹⁶²

¹⁶⁰ Zoom Forms 10-K filed for the United States Securities and Exchange Commission from 2020 to 2023, 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.

¹⁶¹ Backlink, Zoom User Stats: How Many People Use Zoom in 2022? 6 January 2022, URL: <https://backlinko.com/zoom-users>.

¹⁶² Zoom, Form 10-K over 2022 - the fiscal year ending 31 January 2023, URL: <https://investors.zoom.us/static-files/93dbfabb-b7ce-4f51-ba9f-44fe3ebe9c19>

In 2022 (fiscal year ending 31 January 2023), Zoom's revenue had increased to \$4.392,960 million US dollars, compared to \$4.099,864 million USD earned in 2021 and \$2,651.4 million USD earned in 2020. Almost a third of this revenue comes from outside of the US (APAC and EMEA), 30% in 2022.¹⁶³

For its business growth, Zoom relies on word of mouth via viral marketing, and on upselling of its existing customers. *"Our platform is designed to make it easy to host meetings. By attracting free hosts to use our platform, we promote usage that allows hosts and their meeting attendees to experience the Zoom difference. We complement this lead-generation model with our multipronged go-to-market strategy that integrates the viral enthusiasm for our platform with optimal routes-to-market, including direct sales representatives, online channel, resellers, and strategic partners. This approach allows us to cost-effectively drive upgrades to our paid offering and expansion within organizations of all sizes and verticals."*¹⁶⁴

Zoom also writes: *"We see international expansion as a major opportunity".* And: *"With users, offices, and data centers strategically located around the world, we are poised to reach new customers globally. Our platform is intuitively designed such that localization requirements are minimal. For example, our platform works without intensive translation requirements with only a few language adjustments to our user interface and support systems."*¹⁶⁵

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)."*¹⁶⁶

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. It follows that Zoom has a strong economic and financial interest in complying with privacy and security requirements from its EU Education customers.

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

"The markets in which we operate are highly competitive. We face competition from legacy web-based meeting services providers, including Cisco Webex and GoTo, bundled productivity solution providers with video functionality, including Google Workspace and Microsoft Teams, and UCaaS and legacy PBX

¹⁶³ Idem, p. 25.

¹⁶⁴ Idem, p. 6.

¹⁶⁵ Idem, p. 7 and p. 25.

¹⁶⁶ Zoom Answers to DPIA questions, 23 November 2020, Introduction.

providers, including 8x8, Avaya, and RingCentral, as well as consumerfacing platforms that can support small- or medium-sized businesses, including Amazon, Apple, and Facebook.”¹⁶⁷

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.”¹⁶⁸*

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*).¹⁶⁹ 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 were to violate 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.”¹⁷⁰*

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.¹⁷¹

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.”¹⁷²*

¹⁶⁷ Zoom Form 10-K over the year 2022, p. 11.

¹⁶⁸ Zoom Answers to DPIA questions, 23 November 2020, Introduction.

¹⁶⁹ 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>.

¹⁷⁰ FTC and Zoom Consent Order, 9 November 2020, URL: <https://www.ftc.gov/system/files/documents/cases/1923167zoomacco2.pdf>.

¹⁷¹ 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.

¹⁷² Idem.

7.3. Joint interests

The interests of Zoom and the education and research organisations align when it comes to protecting the personal data against unauthorised access with strong security measures. This includes the use of multi factor authentication and the ability to use effective end-to-end encryption. Zoom and its Education 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 has fulfilled its commitment to develop exclusive EU data processing by the end of 2022. This ensures that the personal data from EU customers are protected against direct surveillance in the USA, or in other third countries. In combination with the new adequacy decision for the USA from the European Commission, this measure mitigates all systemic and incidental data transfer risks for the Education end users in the EU. This will be elaborated in Section 8 below.

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 personal against accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access.

8. Transfer of personal data outside of the EEA

8.1. Zoom's factual transfers of personal data

Since the completion of its EU-exclusive data processing by the end of 2022, Zoom no longer systematically transfers personal data from its EU customers to third countries.

Within the EU data boundary Zoom uses a mix of cloud technologies and its own colocated data centres to deliver its services. Zoom's colocation facilities are provided by Digital Realty, Level 3, CoreSite, Aptum, Equinix, Tata, Telstra, Telx, and Zayo. Normally, Dutch Education customers connect with AWS data centres in Germany, but they can connect to any number of colocation sites (data centers), clouds, etc, based on their geolocation (if they travel abroad, or accept participants from these geolocations for example), and their account setup.

Zoom has gradually expanded its EU geolocation offer. At first, Zoom only offered to store a limited subset of the Content Data in data centres in the EU, in Germany. This only applied to meeting recordings, meeting transcripts, in-meeting chat messages, and files exchanged during a meeting. At

the time, persistent chat messages (Team Chat), Account Data, and operation data were still stored in the US.

As shown in Section 4.3.2, Education 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.¹⁷³

Zoom currently uses datacentres in 9 countries/territories.¹⁷⁴ Zoom only incidentally processes personal data from EU Education customers in regions outside of the EU, if an end user travels outside of the EU, if an admin consents to a one-off transfer to get support outside of office hours, in case of a complaint or security flag, or in case Zoom sends a service notification through its subprocessor Twilio from the USA.

Zoom has confirmed in reply to this Update DPIA that it technically redirects its European website 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.

Since early 2023 Zoom also exclusively process the Account, Diagnostic and Support Data in the EU, with the exception of the transfer of limited routing data and the collection of clipped IP addresses in the USA. Only the public Website Data are directly transferred or generated on Zoom's servers in the USA (for which Zoom is a data controller).

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 Education customers to opt in or out of a specific data center region for data in transit.¹⁷⁵

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: (i) if the European Commission adopts an adequacy decision, (ii) if a multinational adopts Binding Corporate Rules, (iii) if an organisation applies the EU Standard Contractual Clauses (SCC), or (iv) if an organisation only incidentally transfers, in an unsystematic way, organisations may also look for a

¹⁷³ Zoom, Protecting your data, URL: <https://zoom.us/trust/security>.

¹⁷⁴ Zoom, Selecting data center regions for meetings and webinars, last updated 10 January 2024, URL: https://support.zoom.com/hc/en/article?id=zm_kb&sysparm_article=KB0060026.

¹⁷⁵ Idem. See also Zoom, Selecting data center regions for hosted meetings and webinars, last updated 10 January 2024, URL: <https://support.zoom.us/hc/en-us/articles/360042411451-Selecting-data-center-regions-for-hosted-meetings-and-webinars>.

transfer legitimation in Article 49 of the GDPR. For Zoom this last ‘incidental transfer’ option is available in six circumstances:

1. If end users travel outside of the EU and participate in Zoom meetings;
2. If admins consent to incidental processing of support tickets in the USA or the Philippines (outside of regular EU office hours), and
3. 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.
4. If Zoom receives a complaint about a user, or its security systems flag a user, the incident is researched by Zoom’s US based Trust & Safety team.
5. For the transfer of the hashed account name with the unique user ID when logging in to Zoom (routing purposes).
6. If a customer integrates a third party application with Zoom, and hence, allows the transfer of Zoom-data to third countries.

Below, the three structural transfer grounds are discussed in more detail.

8.3. European Commission Adequacy decision

An adequacy decision from the European Commission means that the country in question has a level of protection comparable to that applied within the EEA. Since 10 July 2023, there is a new adequacy decision from the European Commission for participants to the EU US Data Privacy Framework (DPF). Zoom has registered as active participant.¹⁷⁶

8.4. 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.¹⁷⁷ These clauses (hereinafter: SCC) contractually ensure a high level of protection.

¹⁷⁶ Data Privacy Framework Program, Zoom listed as active participant since 18 November 2016, URL: <https://www.dataprivacyframework.gov/list> query for ‘Zoom’

¹⁷⁷ 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.

Zoom generally uses the (2021) SCC to legitimise the transfer of incidental personal data from its EU customers to the USA, or the Philippines (for incidental customer support outside of EU office hours). *“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.”* Zoom has since added use of AWS servers in Brazil and Taiwan.¹⁷⁸

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.¹⁷⁹

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. In view of the changes in US surveillance law, transfers to the USA based on the SCCs do not have to be complemented by supplementary measures anymore. The assessment of applicable laws has already been made by the European Commission, meaning that when the SCCs are in place, an additional assessment on top of the SCCs is not necessary.

Though the EU US Data Privacy Framework does not cover the US CLOUD Act (*Clarifying Lawful Overseas Use of Data*), the existence of this law did not prevent the European Commission from granting the adequacy status to the USA. The US CLOUD Act 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.

Hence, SURF continues to rely on the model transfer clauses from the European Commission for the transfer to Zoom Video Communications, Inc in the USA, including the provisions in the SCC that onward transfers to subprocessors have to comply with the same contractual safeguards. The applicable SCC offer a reliable, future proof transfer mechanism that will remain valid even if the DPF would be suspended or invalidated by the European Court of Justice.

¹⁷⁸ Email Zoom in reply to this Update DPIA, 27 February 2024.

¹⁷⁹ Zoom reply to part A of the DPIA, 19 March 2021, p. 13.

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.”¹⁸⁰ 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.”¹⁸¹

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, the previous DPIA put a lot of emphasis on the new possibility to enable E2EE as a means to minimise the risk of unauthorised access by government authorities. The use of E2EE is no longer mandatory to protect sensitive and special categories of data because Zoom processes all data in the EU, and because the remaining risks of unauthorised access by US government authorities are low, according to the European Commission adequacy decision. 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.”¹⁸²

¹⁸⁰ Idem.

¹⁸¹ Zoom, FAQs: Transferring EEA & UK Residents’ Data to the US.

¹⁸² Zoom, Advanced chat encryption, last updated 28 October 2023, URL: <https://support.zoom.us/hc/en-us/articles/207599823>.

Zoom explains the difference between Zoom's regular encryption and E2EE:¹⁸³

"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."

The use of E2EE remains 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."*¹⁸⁴ 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 facilitate access to personal data or systems or for the importer to be in possession of or to hand over the encryption key."*¹⁸⁵

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

¹⁸³ Zoom End-to-end (E2EE) encryption for meetings, last updated 28 October 2023, URL: <https://support.zoom.us/hc/en-us/articles/360048660871-End-to-end-E2EE-encryption-for-meetings>.

¹⁸⁴ Zoom reply to part A of the DPIA, 19 March 2021, p. 84.

¹⁸⁵ Zoom new DPA, Clauses 6.1 and 6.2.

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.¹⁸⁶

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 very useful functionality, but no longer required to prevent risks from the transfer of personal data to the USA.

9.2. Aggregation and anonymisation

According to the guidance from the Data Protection Authorities in the EU, anonymisation is a complex and dynamic form of data processing.¹⁸⁷ 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 initially collects/generates and processes personal data via these log files.

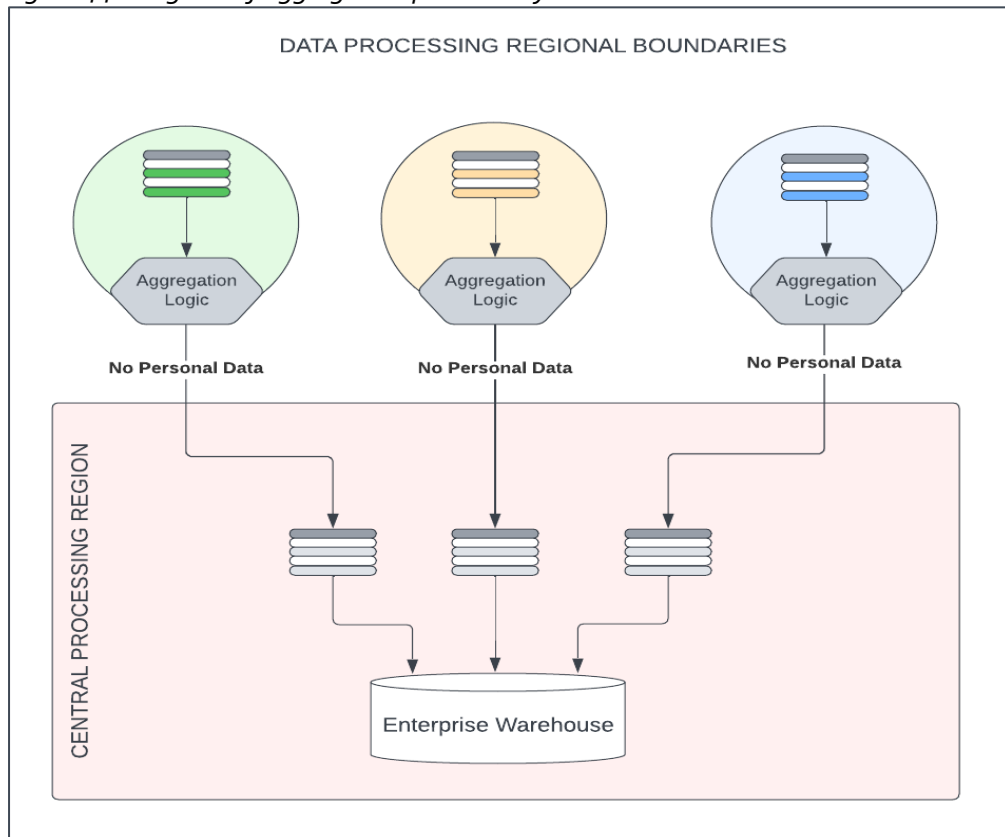
In reply to the first DPIA, Zoom has added a definition of 'anonymisation' to its DPA, stopped using the confusing term 'de-identify', and has agreed to precisely define in the DPA when it may process directly identifiable data, and when only aggregated data. The term 'aggregated' is further specified, that it may never reference to an individual customer (that is, not to a specific university or school).

As part of the ongoing dialogue between SURF and Zoom, Zoom presented different aggregation and masking techniques. The outcome of the discussions was that Zoom chose the strictest type of aggregation for its EU customers: all data are aggregated in the EU, before the unidentifiable statistics are transferred to Zoom's HQ in the USA. See [Figure 44](#) below.

¹⁸⁶ Zoom, Protection your data, URL: <https://zoom.us/trust/security>.

¹⁸⁷ 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.

Figure 44: Diagram of aggregation provided by Zoom



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.

In the DPA 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.¹⁸⁸

¹⁸⁸ Zoom new DPA, Clause 3.2.

Zoom has also committed to comply with the principles of privacy by design and privacy by default (Art. 25 GDPR), and has taken the following specific measures:

- Zoom has implemented 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.¹⁸⁹ Zoom has shown these policies to SURF and Privacy Company.
- Zoom has asserted (and Privacy Company has verified in October and November 2023) that only those cookies which are strictly necessary are set by default for European 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.¹⁹⁰
- When Zoom plans to introduce new features, or related software and services (“New Service”) that will be offered within the scope of the contracted 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.¹⁹¹

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

¹⁸⁹ Zoom new DPA, Clause 3.3.

¹⁹⁰ Zoom new DPA, Clause 3.4.

¹⁹¹ Zoom new DPA, Clause 3.5.

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.

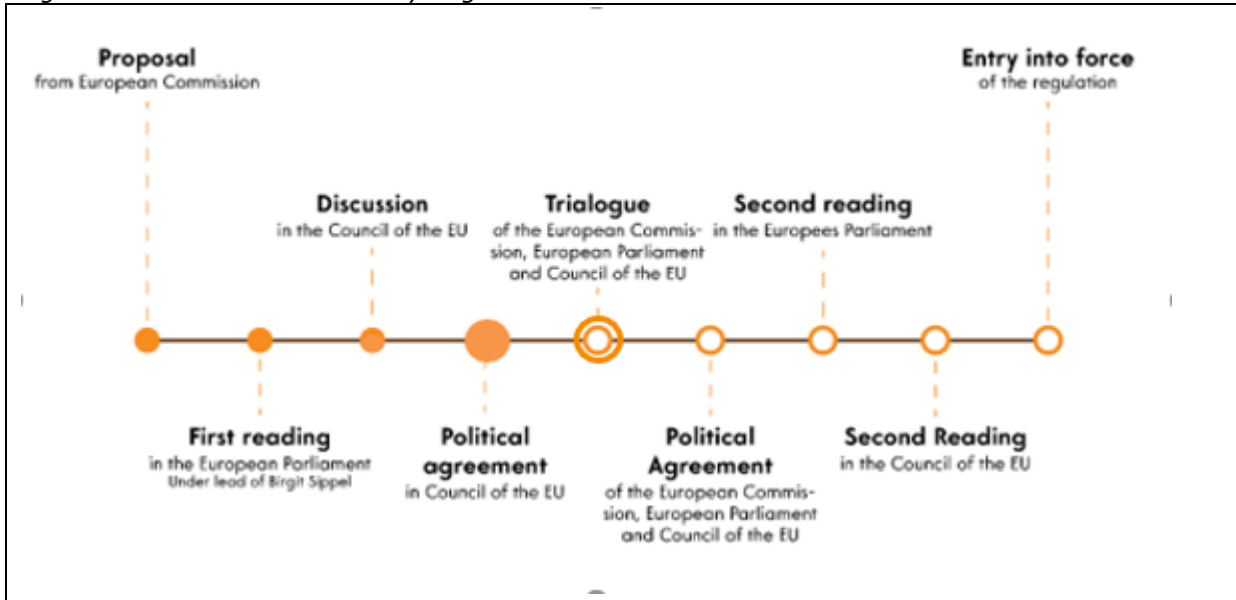
As analysed in Section 3.4 of this report, both the publicly accessible and the restricted access websites only place and read necessary information from end-user devices (cookies and functionally necessary determination of geolocation through the IP address). In reply to the initial DPIA, Zoom has implemented a new cookie consent banner that enables visitors to freely give consent for other, optional cookies. The websites do not set any of these non-necessary cookies if a user doesn't make a choice either. 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 on 27 November 2023, Zoom's cookie practice seems compliant with Article 11.7a of the Dutch Telecommunications Act and with the GDPR requirements 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 if the data are not strictly necessary for the technical functioning of the service. 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 detailed event level information about the telemetry events it collects.¹⁹²

Figure 45: 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 in 2020. 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 7 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

¹⁹² Zoom Meeting, Webinar, and Team Chat Telemetry Events, last updated 1 March 2024, URL: https://support.zoom.com/hc/nl/article?id=zm_kb&sysparm_article=KB0074458.

position to COREPER to start the triologue on 10 February 2021.¹⁹³ The most recent update from the Council dates from 12 November 2021.¹⁹⁴ In the first half of 2022, France announced ePrivacy would be a priority during its Presidency of the Council, but no progress has been booked since.¹⁹⁵ 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 committed to an overhaul of its data retention policy, and to shorten retention periods. Zoom has agreed to retain new data from Dutch university and government customers no longer than 15 months after they sign up for the new DPA, unless otherwise mentioned in the table below.

Zoom has gradually worked backwards to remove all existing older data from all its systems to apply a generalized retention scheme for all its EU 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 4](#) below.¹⁹⁶ Customers can apply their own retention periods to personal data under their control, such as cloud recordings.

Zoom emphasizes: *"This is a point in time assessment. Zoom is in the process of implementing these default retention periods. Zoom actively assesses and adjusts retention timelines to ensure they meet the evolving needs of our customers."* Zoom has published its data retention schedule on 29 March 2024.¹⁹⁷

¹⁹³ 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>.

¹⁹⁴ 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>.

¹⁹⁵ 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/>.

¹⁹⁶ Zoom Data Retention and Deletion Standards for Zoom Accounts purchased by SURF/HEAnet and the Dutch government, Version 1.0, 24 January 2022.

¹⁹⁷ Zoom Meetings, Webinar, and Team Chat Data Retention Standard, 29 March 2024, URL: https://support.zoom.com/hc/nl/article?id=zm_kb&sysparm_article=KB0074786.

Table 4: Zoom data retention periods

Meeting and Webinar Content Data	
Data Type	Timeline for Deletion
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	End user account profile data are retained for as long as the account is active, plus 31 days. Incidentally account data may be retained longer for legal reasons (in case of abuse or fraud). Some information (such as username and display name) and metadata may be retained after the end user account is terminated, if associated with a meeting, chat, webinar of an active user/account.
Hashed e-mail address and unique user identifier of end users, in combination with the chosen geolocation of the customer.	As long as the account is active, only for routing purposes.
Account Holder Business Data (information associated with the individual(s) who are the billing and or sales contact for a Zoom Education or Education account, including: name, address, phone number, email address, billing and payment information, data related to the customer's account, such as subscription plan and selected controls)	These commercial contact data are retained for as long as the account is active plus 10 years after account termination, to meet legal obligations such as tax audits and litigation.
Cloud Recordings (includes closed captioning, live transcripts, recording highlights and chat transcripts)	Information is retained as long as the user has an active account.
Cloud recording raw files ¹⁹⁸	15 days after the date of collection
Polling questions and responses (optional)	15 months from the date of collection
Webinar questions and answers (optional)	15 months from the date of collection

¹⁹⁸ 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.”



Persistent Chat Messages	24 months from the date of collection or as may be otherwise set by customer in their account setting
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 the meeting conversation feature is enabled, retention will follow that of persistent chat messages
Meeting & Webinar registration data	Retained as long as the account is active
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)	Zoom does not store or retain any data server side
Trust & Safety Data	180 days from the date of collection (or 10 years, see above)
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
Sensitive Meeting and Webinar Metadata (user level data) ¹⁹⁹	15 months
Other Service Generated Data that identify individuals	15 months from the date of collection.
Telemetry Data	Up to 15 months from the date of collection
IP addresses (US fiscal law ²⁰⁰)	10 years from the date of collection, but Zoom clips the last octet of IPv4 addresses and the last 64 bits of IPv6 addresses to reduce identifiability.
Website Data	
Data Type	Timeline for Deletion
Zoom web server access log for both public and restricted access website (after log-in)	Up to 12 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/
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.

¹⁹⁹ 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."

²⁰⁰ Based on US Treasury Regulation 1.250(b)-5(e) for services provided to businesses.

Files and images exchanged in both recorded and unrecorded meetings are deleted immediately after the meeting ends.

Zoom stores the cloud recordings as long as the education and research organisation remains a customer of Zoom Meetings Education, plus 15 days after account termination. With Cloud Recordings, Zoom means Mp4 of all video, audio and presentations, M4A of all audio, and audio transcript files. , including chat metadata. Customers can determine a shorter retention period for cloud recordings.

Zoom applies a separate retention period to the data in and from the Team Chat: these data will be deleted 24 months from the date of collection or as early as end users remove messages, files and images from the permanent chat.

Zoom retains other Content Data such as polling questions and responses, webinar questions and answers and webinar registration data 15 months from the date of collection.

Zoom will remove deleted Content Data from its backups 35 days after collection.

11.2. Diagnostic Data

In its data retention table, Zoom describes three categories of diagnostic data, namely:

- | |
|--|
| <ol style="list-style-type: none">1. Meeting or Webinar Metadata2. Telemetry Data3. Other Service Generated Data |
|--|

All three categories are retained for 12 to 15 months after collection. Next to the Meeting and Webinar Metadata, Zoom collects Structured data that is generated by the user when using the service. Zoom will retain these data for 15 months from the date of collection.

Administrators may have access to the following user activity logs in the web portal.

- Admin Activity Logs – 1 month visible, retention determined by the customer
- Sign-in/Sign-out Logs – 1 month visible, longer retention determined by the customer
- Chat History – unknown, was disabled in the test tenant
- Channel Activity Logs – 31 days after collection
- Legal Hold for Team Chat: determined by the customer
- User Disclaimer logs – 1 month
- Reported Participants: retention determined by the customer
- Attendee Logs – 180 days after collection
- Requests of accessing content –determined by the customer

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 includes data that, for example, is maintained in infrastructure logs.”* Such logs are retained for 31 days after collection/generation.

Zoom will retain Security logs for 24 months after creation/collection.

As mentioned in Section 5.2.2 Zoom is legally required to retain IP addresses from its EU customers for a period of 10 years, to validate customer location. Even though the retention period determined by US fiscal law is 6 years, Zoom explained that it must retain for 10 years to comply with demands from European tax authorities, as the statute of limitations for electronically supplied services in the EU is 10 years. *“Second, Zoom may need the data to respond to the United States Internal Revenue Service, which may ask that Zoom prove it does not engage in tax fraud, and to provide data for more than six years (but likely not exceeding ten). And third, there are instances where Zoom will need to enter or has already entered into an agreement with the IRS (or another foreign tax authority) to extend the statute of limitations. For at least these reasons, Zoom retains clipped IP addresses for 10 years rather than 6 years.”*²⁰¹

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.

Account Holder Business Data: Zoom (as an independent data controller) retains the sales and billing contact data as long as the account is active plus 10 years to meet legal obligations, such as tax audits and litigation..

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. Zoom has also developed a ‘deletion’ option in the Privacy section of the admin portal. This option also removes the Diagnostic Data from that user to the extent possible. Some information (such as username and display name) may still be retained in other Diagnostic Data for up to 14 months if associated with a meeting of another active user’s account. Incidentally account data may be retained longer for legal reasons (in case of abuse or fraud). Some information (such as username and display name) and metadata may be retained after the end user account is terminated, if associated with a meeting, chat, webinar of an active user/account.

²⁰¹ Mail Zoom in reply to this Update DPIA, 27 February 2024.



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.

As described in Section 3.4, Privacy Company verified that Zoom has limited the use of cookies by subprocessors in the service provided to SURF.

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.”*²⁰²

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 education and research 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 education and research organisations as controllers, when Zoom is a processor. Additionally, through the DPA, EU Education 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 authorised data controller for these six purposes.

²⁰² 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.

The legal ground of vital interest is not discussed, since neither Zoom nor education and research organisations have a vital (lifesaving) interest in processing personal data via Zoom Meetings.²⁰³ 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.²⁰⁴

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, education and research organisations can successfully appeal to four of the six possible legal grounds. These are discussed below.

²⁰³ Of course, a university or research institution 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.

²⁰⁴ Zoom new DPA, Clause 2.2.

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 institutions and students, consent can seldom be given freely.²⁰⁵ 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 education and research institutions 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.”*²⁰⁶

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 Education end user in their Zoom account. Education and research 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 education and research organisations can only rely on the legal ground of consent for the processing of some Content and Account Data for three purposes:

- | |
|---|
| <ol style="list-style-type: none"> 1. (For admins) Subscribe to mailing lists with announcements related to software updates, upgrades, and system enhancements, |
|---|

²⁰⁵ 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.”

²⁰⁶ EDPB, *Guidelines on consent*, paragraph 3.1.1.

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.”*²⁰⁷

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, education and research 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 education and research 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 education and research institution, 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.

²⁰⁷ Zoom new DPA, Clause. 2.6.

Generally, education and research 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, education and research organisations may also invoke the legal ground of the performance of their public tasks.²⁰⁸

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).

²⁰⁸ 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.

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. Since February 2022 Zoom has 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 education and research 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 authorised data controller

As discussed in Section 6.4, Zoom as a data controller can legitimately process some (limited) personal data for its own business purposes, when the processing is necessary. The Dutch research and education 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 6.4 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,
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.²⁰⁹

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

²⁰⁹ Zoom new DPA, Clause 2.4.

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 interests

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:

- | |
|---|
| <ul style="list-style-type: none">a) the link between the collection and the further processing,b) the relationship between the end users and Zoom,c) the sensitivity of the data,d) the possible consequences of the processing, ande) 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 education and research organisations 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.

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.
3. The retention period of maximum 12 to 15 months for Diagnostic and Support Data
4. Zoom's commitment to comply with the five conditions for disclosure (see Section 6.4.1), including the commitment to legally fight every order (with or without a non-disclosure order) specifically aimed at EU 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 validly compelled to disclose personal data to law enforcement and security services and not allowed to redirect the order to its customer.

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 voluntarily detect, remove and report child sexual abuse online for a period of three years.²¹⁰ This (temporary) Regulation entered into force on 2 August 2021, and will expire on 24 August 2024.

Meanwhile the European Commission tried to create permanent rules for CSAM scanning, including obligations to build backdoors for law enforcement. Its proposal for a (permanent) Regulation from

²¹⁰ 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.

May 2022²¹¹, has met with so much public resistance²¹² that it still is pending. On 1 December 2023, the European Commission proposed an extension of the interim regulation for a period of maximum 2 years.²¹³

The EDPB and the EDPS have adopted a common and highly critical opinion on this proposal on 28 July 2022.²¹⁴ They for example write: *“The EDPB and EDPS also express doubts regarding the efficiency of blocking measures and consider that requiring providers of internet services to decrypt online communications in order to block those concerning CSAM would be disproportionate. Furthermore, the EDPB and EDPS point out that encryption technologies contribute in a fundamental way to the respect for private life and confidentiality of communications, freedom of expression as well as to innovation and the growth of the digital economy, which relies on the high level of trust and confidence that such technologies provide.”*²¹⁵

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

²¹¹ Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL laying down rules to prevent and combat child sexual abuse, Com/2022/209, URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2022%3A209%3AFIN>.

²¹² See for example the Open letter from 81 NGOs coordinated by European Digital Rights (EDRI): EU countries should say no to the CSAR mass surveillance proposal, 13 September 2023, URL: <https://edri.org/our-work/open-letter-eu-countries-should-say-no-to-the-csar-mass-surveillance-proposal/> and the open letter from 465 researchers and scientists, at <https://docs.google.com/document/d/13Aeex72MtFBjKhExRTooVMWN9TC-pbH-5LEaAbMF91Y/edit?pli=1>.

²¹³ European Commission press release, Commission proposes to extend Interim Regulation allowing providers to continue voluntary detection and reporting of child sexual abuse, 1 December 2023, URL: https://ec.europa.eu/commission/presscorner/detail/en/mex_23_6242.

²¹⁴ EDPB-EDPS Joint Opinion 4/2022 on the Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse, URL: https://edps.europa.eu/system/files/2022-07/22-07-28_edpb-edps-joint-opinion-csam_en.pdf

²¹⁵ Idem, p. 6 (Summary).

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 education and research 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 (in an EU data centre).

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 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.

There are high data protection risks for end users if special categories of personal data would be breached: either by malevolent or blackmailed employees of Zoom or the education/research organisation, or by external hackers, by state actors, or as a result of an order from a government authority for compelled disclosure.

To prevent this high risk, organisations are (still) advised to enable to encrypt Content Data with E2EE and Advanced Chat if they know that special categories of data are exchanged via Meetings.

To further mitigate the risks relating to unauthorised access to the metadata, education and research 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, 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 education and research 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 education and research 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 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.²¹⁶ 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.²¹⁷ Zoom has recently published a better explanation of the DSAR results in its public Help article, and provides a more understandable output, grouped by product.²¹⁸ Last but not least, Zoom has revised and updated its data retention policy. As detailed in Table 4, 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 committed to improve access to individual personal data, by developing three new take-out tools. These were: (i) an improved take-out for admins of all personal data relating to a specific data subject (realised by the end of 2022), (ii) a self-service take out for data subjects to file Data Subject Access Requests (to be realised by the end of 2024), and (iii) a take-out of admin behaviour (to check administrator compliance with policy rules, observed by Privacy Company on 3 November 2023). These take-outs compensate for the fact that there is no easy access to the Telemetry Data and Webserver access logs yet , 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, the commitment to make a Diagnostic Data Viewer available in the first half of 2024, and the remaining commitment to create a unified response to a DSAR request by the end of 2024, 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).²¹⁹ 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

²¹⁶ Zoom, Privacy Data Sheet, last updated April 2023, URL: <https://explore.zoom.us/media/privacy-data-sheet.pdf>.

²¹⁷ Zoom Cookie Statement, last updated 30 June 2023, URL: <https://explore.zoom.us/en/cookie-policy/>.

²¹⁸ Zoom, Using Data & Privacy for data management, URL:https://support.zoom.com/hc/nl/article?id=zm_kb&sysparm_article=KB0057736 .

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 public website, and minimisation of data retention periods. Zoom contractually agrees to perform a DPIA before introducing new features or related software and services. As described in Section 5.2.2. Zoom has also applied privacy by design to the creation of business statistics. Zoom has chosen the most restrictive model, whereby it aggregates all EU data in the EU, before transferring the statistics about daily and monthly active users to the USA.

Zoom notably failed to apply the principle of privacy by design with regard to the processing of its public 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, both the restricted and publicly accessible Zoom websites were found to comply with both the ePrivacy and GDPR transparency and consent requirements. European Education customers can also use their own vanity subdomain for the log-in, 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. 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 to 15 months (with some exceptions described in the table) or, as long as the contract lasts with the end user or the education/research organisation, plus a back-up of 31 days. With this data retention policy Zoom's processing meets the proportionality requirements.

Fiscal rules, both in the US and in the EU, require service providers that wish to benefit from tax deduction to provide evidence where income is earned, based on the location of the end users. Because of these rules, Zoom is required to retain IP addresses for a period of 6 to 10 years. Zoom has decided to clip the last octet from the IPv4 addresses, and the last 64 bits of IPv6 addresses to reduce identifiability, and retains these IP addresses in a separate container for a period of 10 years. Zoom has assured SURF that *“access to clipped IP addresses is role based and highly restricted, limited to a small number of Zoom employees, in accordance with Zoom’s access control policies and standards.”* Zoom has also informed SURF that it has so far not disclosed any data to fiscal authorities. If Zoom would receive such a request *“We would only provide clipped IP addresses after exhausting all other options and only if the Tax Authority has basis to request it.”*²¹⁹ Finally, Zoom has assured SURF that it will further reduce identifiability of the IPv6 addresses by clipping the last 80 bits.

15.3. Assessment of subsidiarity

When making an assessment of subsidiarity, the key question is whether education and research organisations can reach the same objectives (of using secure, bug free, modern videoconferencing, chat and file exchange software), with less intrusive means.

Education and research 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 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.

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 education and research 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 customers in the EU. Sections 16.2 to 16.7 analyse whether data subjects can effectively exercise each of these rights.

²¹⁹ E-mail Zoom in reply to this Update DPIA, 12 March 2024.

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. Since Zoom has become a data processor for the 5 relevant categories of personal data, its customers (via SURF and the Dutch government) must comply with the obligation for data controllers to provide information and to duly and timely address these requests. The tailored data processing agreement with Zoom includes obligations to assist the data controller in complying with data subject rights requests.

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 updated 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.” ²²⁰

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, and has not yet completed its Telemetry Viewer (to be delivered before July 2024). After some discussions with Privacy Company, Zoom did provide information from its three kinds of server logs (Meeting Logs, Event Logs (with the Telemetry Data) and Account Logs), and some Website Data.

Zoom has committed to provide full access to all available personal data, through three new take-out tools. Two of these tools are already available (access to end user and admin data via the admin portal), the third one (DIY portal for end users) will become available by the end of the 2024.²²¹ As described in Section 3.3, in November 2023 Zoom provided access to many data relating to the test user via the admin interface, but the presentation of these results in different files with meaningless names was incomprehensible. It is plausible that Zoom has a legitimate interest to protect itself against reverse engineering, but this can never legitimise undermining of the fundamental right of data subjects to obtain the personal data *“in an intelligible and easily accessible form, using clear and plain language”* (Article 12 GDPR).

In the dialogue with Privacy Company and SURF Zoom acknowledged that randomizing table names/file names for security reasons was not helpful for data subjects that filed a DSAR. Zoom agreed to improve the understandability of the output, and has recently improved the relevant Help article with information about the contents of the different files.²²² Zoom also provides a more understandable output, grouped by product.²²³ To make access more easily available, the new Do It Yourself access tool for end users will become available before the end of 2024.

Zoom agrees that access through the self-service tool for end users should include access to identifiable data from its public and restricted access Website request logs. Zoom can only rely on the

²²⁰ Zoom new DPA, Clauses 8.1 and 8.2.

²²¹ The 3 tools are: (i) 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.

²²² Zoom, Using Data & Privacy for data management, last updated 27 February 2024, URL:

https://support.zoom.com/hc/en/article?id=zm_kb&sysparm_article=KB0057736

²²³ Zoom sent a sample of the new DSAR output on 27 February 2024.

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 education and research institutions 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 15 months from the date of collection, or as long as an organisation remains a customer. 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.

Some retention periods are determined by Zoom for its own legitimate interests: such as webserver access logs, security logs, IP-addresses to comply with US fiscal law, and retention of individual data in case of abuse, complaints or a legal procedure.

Based on the requirements of Article 17(1)(a) and Article 17(1)(d) of the GDPR, education and research 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 has developed a data deletion tool for admins since the end of 2022.

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 also have “*the right not to be subjected to an exclusively automated decision if it has legal effects, including profiling.*” (Article 22 (1) GDPR).

Based on 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.”²²⁴

This prohibition also extends to guest users. Even when they participate in a Meeting hosted by an EU Education customer with a ‘free’ account, which can include advertising²²⁵, 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 launched a self-service Marketing Communication Preference Center. This enables all users, including Zoom’s commercial contacts, to subscribe or unsubscribe from different mailing lists.

With regard to profiling Zoom is required based on US law to scan some Content Data for child abuse material. As explained in Section 12.2.1, since 6 July 2021, such data processing is permitted in the EU, based on a temporary derogation of the ePrivacy rules (valid until August 2024). As analysed in Section 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:

²²⁴ Zoom new DPA, Clause. 2.5.

²²⁵ 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/>.

“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.”²²⁶

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 education and research institutions 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 its customers to help them with data portability requests from its employees and students.

16.7. Right to file a complaint

Finally, as data controllers education and research 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 (education and research organisations) can honour the rights of data subjects. Zoom has already made the DSAR output more understandable by publishing information about the contents of the different files, but Zoom has also committed to further improve on the accessibility and understandability of the DSAR results by creating a DIY portal for end users to file DSARs, and by rearranging the DSAR results in a unified format.

²²⁶ Zoom new DPA, Clause. 2.7.

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 may result 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 Zoom has agreed with its EU Education 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 customers. They have access to audit log files and reports with information about individual user activities. Education and research organisations could potentially combine information from these log files to create a (performance) profile of Zoom end users. The knowledge that employers (education and research 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.²²⁷ Education and research organisations can mitigate these risks by adopting clear policy rules to prevent the use of the log files for employee evaluation purposes. Because Zoom has also created access to logs of

²²⁷ Merriam-Webster Online Dictionary, "chilling effect", URL: https://www.merriam-webster.com/legal/chilling_effect

admin behaviour, organisations can use these logs to audit that admins have not misused access to the personal data 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 and special categories of data by using Zoom Meetings. For example, employees may discuss sensitive financial data in relation to subsidies, exchange health data to explain absence from work, or exchange files with data about crimes or convictions. Such sensitive personal data 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, such data can become part of the Diagnostic Data.

Even though Zoom already exclusively processes streaming data of its EU customers and the contents of Support tickets in data centres in the EU, access to these data can be ordered through US legislation such as the US CLOUD Act. In view of the new adequacy decision for the USA, application of E2EE is no longer required to mitigate transfer risks. However, from a security perspective E2EE is advised to mitigate risks from possible data breaches. Zoom offers this protection for all streaming data and chats.

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 disadvantage²²⁸

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.”*²²⁹

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 due to unauthorised access to Content Data

The previous version of this DPIA already concluded, based on a detailed risk calculation in the DTIA, that the likelihood is very small that Zoom will be compelled to disclose Content Data to government authorities. The risk calculation was based, amongst others, on Zoom’s contractual promises to legally resist all orders that are specifically targeted at EU Education customers, its transparency reporting, short data retention periods and the creation of an exclusive EU cloud for almost all personal data.

Since June 2023, the risk of unauthorised access by US authorities is mitigated by the new European Commission adequacy decision for the USA. This DPIA assumes Dutch education and research organisations won’t change the default setting that the Content Data processing takes place in Zoom’s EU data centres. The adequacy decision means the mitigating measure of encryption with a self-controlled key of the Content Data is no longer required for transfers to the USA.

Even though the probability of occurrence of the risk of compelled disclosure to government authorities is extremely low, the data can also be breached by malevolent or blackmailed employees

²²⁸ 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/>.

²²⁹ Idem.

of Zoom or the education and research organisation, by external hackers, by state actors, or as a result of an order from another government authority for compelled disclosure. The impact on data subjects of such breaches on data subjects can be extremely high, especially when it involves special categories of data.

Therefore, organisations are advised to use Zoom's E2EE for Meetings and chats, including exchanged files, especially when special categories of data are exchanged. This means that even if the data are breached, the recipients 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.

To further mitigate risks of unauthorised access to Content Data, organisations should carefully consider the options to minimise processing of Content Data as part of the metadata. Depending on the sensitivity and confidentiality of the data, they may want to apply measures such as a policy about the naming convention of Meetings and Rooms, and take additional data minimisation measures, such as using Single Sign On to provide Zoom with pseudonyms.

Assuming the organisations with Zoom Education licenses take the recommended mitigating measures, the probability of occurrence of this data breach risk is low. Even though the impact on data subjects of a breach could be high, the risks for data subjects can be qualified as low.

17.2.2. Loss of control, loss of confidentiality through transfer of personal data to the USA and the Philippines

Even though Zoom processes all metadata exclusively in EU data centres, Zoom structurally and incidentally transfers some personal data to the USA: structurally for operational and security purposes, and in 5 specific exceptional situations (Trust & Safety, use of Zoom outside of the EU, support outside of EU office hours, use by organisations of third party applications, and when Zooms sends service notifications through its USA subprocessor Twilio).

Zoom systematically transfers pseudonymised Account and Diagnostic Data to the USA, for routing purposes. The transfer of the hashed mail address with the unique user identifier to the USA is necessary to identify the user and rout the user to the proper geolocation.

Zoom incidentally transfers Diagnostic Data to its central Trust & Safety Team in the USA. The transfer of incidental Diagnostic Data to the USA is necessary to identify and block bad actors that threaten the security and integrity of Zoom Services. These data are accessible only by Zoom employees with a need to know and subject to appropriate technical and organisational measures. The transfer should only involve pseudonymous identifiers, no Content Data or readable user names. 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.

Additionally, Zoom can incidentally transfer some personal data to the USA if an end user travels outside of the EU, and to the USA and the Philippines if an admin consents to a one-off transfer to get support outside of office hours.

The fourth type of incidental transfer is when a customer decides to use integrations with third parties that may transfer personal data to the USA, such as Giphy and Twilio (invite mailings for webinars). Organisations are advised not to enable Giphy, and to use their own GDPR-compliant subprocessors to send invitations for Zoom webinars. If the organisation nonetheless uses Zoom's subprocessor Twilio for mailings, they should disable the tracking pixel to prevent an additional risk of loss of control due to the secretive observation of e-mail interaction behaviour (opening, reading, forwarding). Zoom itself has also disabled the tracking pixel for its service notifications.

The final fifth type of incidental transfer is when end users receive service notifications from Zoom through subprocessor Twilio, for example when they forgot their password, and ask for a reset.

Public sector organisations can mitigate the risk of the systematic transfer of the hashed mail addresses with the user identifier by using Single Sign On. That means Zoom will only have access to a tokenised e-mail address.

Public sector organisations can mitigate the risks of the incidental transfers by informing their employees and students about the transfer risks when they use Zoom outside of the EU. If necessary, they can perhaps use a VPN to connect to the EU data centres. The risk of incidental transfer of support requests can be mitigated by drafting an instruction for admins when they can consent to export of Support Data to the USA and the Philippines, defining the exceptional emergency circumstances that justify use of the support desk outside of EU office hours.

Assuming the public sector organisations with Zoom Education licenses take the recommended mitigating measures, the probability of occurrence of the risk is low. Even though the impact on data subjects of unauthorised access by government authorities in the USA and the Philippines could be high, the risks for data subjects can be qualified as low.

17.2.3. Lack of transparency applicable privacy rules

If organisations do not create a tailored log-in process for their users, Zoom will show all users the same sign-up screen, with a reference to Zoom's general Privacy Statement and Terms of Service (See [Figure 2](#) in [Section 1.3](#)). This information is incorrect, and could put Dutch public sector on the wrong foot about the privacy conditions for the use of the service. Organisations can mitigate this risk by using a Vanity URL like `universityofamsterdam.zoom.us` in combination with Single Sign On (SSO). That way, they can show the organisation's own privacy policy and use conditions during sign-up, and on

all meeting, webinar, and recording registration pages. This has the added benefit that Zoom only has access to tokenised e-mail addresses for routing purposes.

Alternatively, if the organisation does not use SSO and end users must individually sign-up: tell them Zoom's general (consumer) privacy statement and TOS do not apply.

An added benefit of the use of a vanity URL is that organisations can also make guest users aware of the house rules for the use of Zoom services.

Assuming the public sector organisations with Zoom Education licenses take the recommended mitigating measures, the probability of occurrence of the risk is low. Even though the impact on data subjects could be medium, the risks for data subjects can be qualified as low.

17.2.4. Difficulty to exercise Data Subject Access Requests

At the start of this DPIA process, Zoom qualified itself as data controller and did not provide the requested overview of all personal data it processed, in reply to a Data Subject Access Request (DSAR). In a second, more extensive reply to the DSARs, Zoom did provide more Diagnostic Data, including Telemetry Data.

As a result of the negotiations with SURF, Zoom has agreed to become a data processor, and has developed an interface for admins to answer DSARs from their users. As described in [Section 3.3](#), and analysed in [Section 16.3](#), this tool provides a lot of output, but the presentation of these results in different files with meaningless names was incomprehensible. This does not allow controllers to provide the personal data to students and employees *"in an intelligible and easily accessible form, using clear and plain language"* (Article 12 GDPR). Zoom has improved the understandability of the DSAR output with explanations in the public Help article about the Data & Privacy menu.²³⁰ To make access more easily available, Zoom will make a new Do It Yourself access tool for end users available before the end of 2024, with a more logically grouped file of personal data.

In view of these commitments and improvements, data subjects can exercise their fundamental privacy rights. Even though the impact on data subjects is automatically assessed as high, because of the impossibility to exercise a fundamental right, the privacy risks for data subjects can nevertheless be qualified as low.

17.2.5. Employee monitoring system: chilling effect

Admins of education and research 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

²³⁰ Zoom, Using Data & Privacy for data management, last updated 27 February 2024, URL: https://support.zoom.com/hc/en/article?id=zm_kb&sysparm_article=KB0057736

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.²³¹ However, Zoom has developed a DSAR tool 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.

Average workers spend considerable amounts of work time using videoconferencing tools. That makes processing for such employee evaluation purposes more plausible. The knowledge that employers (education and research organisations) can process the Diagnostic Data for profiling purposes can cause a *chilling effect* on employees and students of the Zoom Meeting services. 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 education and research organisations 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 probability of occurrence of the risk is low. Even though the impact on data subjects could be high, the risks for data subjects can be qualified as low.

17.3. Summary of risks

These circumstances and considerations as explained above lead to the following five low data protection risks for data subjects:

1. Loss of control and loss of confidentiality due to unauthorised access to Content Data

²³¹ Zoom, Attendee attention tracking, last updated 15 December 2021, URL: <https://support.zoom.us/hc/en-us/articles/115000538083-Attendee-attention-tracking>

2. Loss of control and loss of confidentiality through transfer of personal data to the USA and the Philippines
3. Lack of transparency applicable privacy rules
4. Difficulty to exercise Data Subject Access Requests
5. Employee monitoring system: chilling effect

For all of these risks, the impact on data subjects may vary from minimal impact to serious harm. In the table below, the highest impact is chosen.

Based on the ICO model, this results in the following matrix:²³²

Severity of impact	Serious harm	Low risk 1, 2, 4, 5	High risk	High risk
	Some impact	Low risk 3	Medium risk	High risk
	Minimal impact	Low risk	Low risk	Low risk
		Remote	Reasonable possibility	More likely than not
		Likelihood of harm (occurrence)		

²³² 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 education and research organisations.

18. Risk mitigating measures

Section 17.2 of this report describes five potential low risks for data subjects. Education and research organisations can prevent these risks by following the recommended measures.

Table 5 below shows the recommended mitigating measures for education and research organisations.

Table 5: Overview of recommended measures for organisations

Low risks	Measures Education & Research institutions
Loss of control, loss of confidentiality due to unauthorised access to Content Data	Consider enforcing the use of E2EE as a good security measure. This is no longer required to mitigate data transfer risks.
	Consider use of the available privacy options such as: <ul style="list-style-type: none"> • 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 • Enable the waiting room for participants
	Create policy rules to prohibit the use of confidential data in room and topic names. If necessary for internal confidentiality requirements: draft a policy to instruct users if they can or must use a profile pictures.

Loss of control, loss of confidentiality due to incidental transfer of personal data to third countries	Organisations are advised to carefully assess optional third party integrations offered by Zoom, not enable Giphy, and use their own GDPR-compliant subprocessors to send invitations for Zoom webinars. If the organisation uses Zoom’s subprocessor Twilio to send webinar invitations: do not enable the tracking pixel, or ask for prior unambiguous consent for this tracking from the recipients, provided that the recipients are legally able to freely give such consent (difficult for employees).
	Enable (or do not disable) ‘EU-only’ for Support requests. Draft an instruction for admins when they can consent to export of Support Data to the USA and the Philippines in exceptional emergency circumstances outside of EU office hours.
	Use Single Sign On to further reduce the transfer risks of pseudonymised e-mail addresses to Zoom in the USA (necessary when logging-in).
Lack of transparency Account and Diagnostic Data	Use the Vanity URL like universityofamsterdam.zoom.us in combination with Single Sign On (SSO) to be able to show the organisation’s own privacy policy and use conditions during sign-up, and on all meeting, webinar, and recording registration pages. Alternatively, if the organisation does not use SSO and end users must individually sign-up: tell them Zoom’s general consumer privacy policy and TOS do not apply.
Difficulty to exercise Data Subject Access Requests	Zoom has developed a self-service tool for admins. Inform parents, students and employees how they can file a data subject access request with the school or university administrator. By the end of 2024, end users should be able to file a DSAR directly, via a new DIY portal. Zoom will also release a Diagnostic Data Viewer for the Telemetry Data before June 2024.
Employee monitoring system	Create a policy to prevent abuse of audit logs and reports as an employee and admin monitoring tool
	Regularly check the logfiles with admin behaviour to verify compliance

Conclusions

Zoom has taken most of the agreed measures to mitigate the remaining low data protection risks, and will take the two remaining agreed measures by the end of 2024 at the latest.

Zoom now processes most of the personal data from Dutch Education customers exclusively in the EU. Zoom does not systematically transfer personal data to third countries outside of the EU, only incidentally, if an end user travels outside of the EU, if an admin consents to a one-off transfer to get support outside of office hours, in case of a complaint or security flag, or in case Zoom sends a service notification through its subprocessor Twilio from the USA.

Zoom does systematically transfer pseudonymised account data and IP addresses to the USA, but because of the new EU adequacy decision for the USA in July 2023, and because Zoom is a participant to the EU US Data Privacy Framework, there are no more high risks resulting from these data transfers to the USA. **If the Dutch education and research organisations apply the recommended measures, there are no known data protection risks for the individual users of the Zoom videoconferencing services.**