Data Transfer Impact Assessment (DTIA) on the transfer to third countries of Content Data processed by Google Meet (audio/video conferencing)

Note: this tab describes the transfer of Content Data. Google uses the term Customer Data in its public data processing agreement for cloud services. URL: https://cloud.google.com/terms/data-processing-addendum. Google's category of Customer Data includes the contents of information shared by customers as Support Data, but not the Account Data, even though they are provided by customers themselves. Because there are differences in both the impact and the probability of unauthorised access to the different personal data, this DTIA continues to distinguish between 6 categories of personal data, and describes both the content of support requests, and the meta data about the requests as Support Data. This distinction also make this DTIA more comparable with other public DTIAs on videoconferencing services.

Step 1: Describe the intended transfer

			COMMENTS GOOGLE OR PRIVACY COMPANY
a)	Data exporter (or the sender in case of a relevant onward transfer):	Dutch education and research organisation [X]	
b)	Country of data exporter:	**[Confidential]** for the Dutch education sector.	Technically, Google maintains servers around the world and its support and service engineers in the 7 third countries can access data anywhere, if necessary and authorised.
c)	Data importer (or the recipient in case of a relevant onward transfer):	Google LLC in the USA. The Dutch education customers rely on appropriate transfer mechanisms under Chapter V GDPR.	
d)	Country of data importer:	USA, with onward transfers to third countries. The contracting entity for Dutch education customers of Google Workspace is **Google Cloud EMEA Limited** (see https://cloud.google.com/terms/google-entity), a Google entity based in Dublin, Ireland. Google Cloud EMEA Limited is a wholly owned subsidiary of Google LLC, which in turn is a wholly owned subsidiary of Alphabet Inc.	
e)	Context and purpose of the transfer:	Google Meet (https://apps.google.com/intl/en/meet/) provides the ability to organise and participate in video conferences, which can consist of 1-on-1 or group calls (up to 500 participants) with both audio and video or just audio. The video conference service also offers related features such as text chatting and file sharing among participants, (AI generated) live captions of speech, and (AI) translations of live captions. This tab is about the transfer of both the live streaming and processing of recorded/stored Content Data, including Content Data in shared files and the chat. Content Data may be stored in or accessed from multiple third countries and the United States. In its Data Transfer policy Google writes: "We maintain servers around the world and your information may be processed on servers located outside of the country where you live." URL: https://policies.google.com/privacy/frameworks. In its subprocessor documentation, Google explains that there are two kinds of transfer: (1) for support and (2) (a) for data centre operations, (b) service maintenance and (c) technical support. 1. If a customer asks for support, and explicitly elects to enable access to recorded meetings in the course of a support case (e.g., by granting access to a Google Doc, Google Sheet, or Google Drive folder). In that case, the Content Data may be transferred to 12 third countries (without an adequacy decision from the EU): Australia, Brazil, Chile, El Salvador, Guatemala, Hong Kong, India, Malaysia, Mexico, Philippines, Singapore and Taiwan, plus the USA. 2. Google does not access any personal data for the first sub purpose of data centre operations. For the second and third sub purpose Google engineers in all locations have limited, authorized access to (recorded) Customer Data for troubleshooting of all kinds of technical issues, releasing new code, making configuration changes or emergency maintenance purposes as well as mitigation of customer-initiated support requests. Google uses subprocessors in 7 third countries that may have access to the Content Data: Australia, Brazil, Chile, Hong Kong, India, Singapore and Taiwan. Additionally, access may be obtained from the USA. See https://workspace.google.com/terms/subprocessors.html for Google's public documentation. Google has provided confidential information relating to its subprocessors and affiliates to SURF and SIVON. Google has explained the probability of this transfer is very low: "Google service maintenance engineers located in Australia, Brazil, Chile, Hong Kong, India, Singapore, or Taiwan have not accessed any Google Meet Customer Data or Service Data	Note Privacy Company: Google does not ask for specific consent for the transfer of Content Data to employees in the first list of 12 third countries: the support employees only ask for consent to access to Content or Service Data of the customer without informing the customer in what country they operate. **That is why this DTIA assumes that schools and universities will not provide such consent**.
f)	Categories of data subjects concerned:	Google Workspace administrators, students and employee users of Dutch education and research organisations + external participants in Meet conferences (as guest users, or with a Google account).	
g)	Categories of personal data transferred:	The streaming and recorded Content Data may include any type of regular, sensitive or special categories of data, and the legally protected category of national identity numbers, depending on the nature of the conference.	
h)	Sensitive and special categories of personal data:	In a teacher-parent conference special categories of data may be exchanged about special needs of a child. In a conference between for example the Dutch police and a citizen, data relating to criminal offenses may be exchanged. Participants can exchange all kinds of personal data via the chat and via file sharing. These sensitive/special categories of data may end up in recordings and transcripts of conferences.	
i)	Technical implementation of the transfer:	Google allows its Workspace for Education Plus customers to select datacentres in the EU to store the recorded Content Data from Meet. See: Google, Data regions: Choose a geographic location for your data, URL: https://support.google.com/a/answer/7630496?hl=en. Google explains that the covered data in the data region policy include meet recordings, including chats (.SBV files), in Drive. Other covered data includes attendance reports, polling results, transcripts, questions, the submitter of question, and Jamboard. All other data such as streaming data, Account Data, Support Data, Diagnostic Data and Website Data are not covered by the geolocation choice. Education customers of the 'free' Fundamentals Workspace versions do not have a data residency choice. This means the recorded Content Data may be transferred to 12 third countries plus the USA if they ask for support and allow access to the recorded Meet data. This DTIA assumes that schools and universities will select the EU as data region, and will not provide consent for such access if it involves transfer to the 12 third countries. As described in row 8, Google's subprocessors may access the recorded Content Data in 7 third countries when this is necessary for service maintenance purposes and to respond to customer-initiated requests, even if a customer does not grant explicit consent for such access in relation to a support request. Google is "on schedule" with its publicly announced expansion of the data region choice for Workspace for Education Plus customers with access controls to prevent access for support outside of the EU, processing-in-region along with an in-country copy by the end of 2023. See: https://workspace.google.com/blog/product-announcements/announcing-sovereign-controls-for-google-workspace. The data region choice does not cover the transient data processing during the live conference calls. This means the streaming data can be processed by all global Google datacentres. Google has explained that there is no administrative access from Google to in-progress meetings, because non-invitees are prohibited from joining.	
j)	Technical and organizational measures in place:	**Technical measures:** Google offers Client Side Encryption (CSE) for Meet. This is available for browsers (including Chromebooks), on Android and iOS smartphones. However, In view of the current complexity of CSE, financial and organisational hurdles to implement CSE, and Google's warnings to end users that many desired functionalities won't work, this DTIA assumes that Dutch schools and universities do no use CSE for day to day use. The second technical measure applied by Google is use of its own encryption in transit for inter-region data traffic and global routing (ALTS and TLS, plus the MTA-STS standard for mail), and AED for data stored at rest. A third technical measure available for Workspace customers with a paid license is the additional protection of Access Approval to explicitly approve access to recordings and transcripts stored in Drive. **Organisational measures:** Google has provided contractual guarantees to the Dutch Education customers that sub-processors may only process personal data in accordance with the framework agreement, and that this guarantee applies to both the Content Data and the Diagnostic Data (Service Data). Google writes: "Before onboarding a subprocessor, Google conducts an audit of the security and privacy practices of the subprocessor to ensure the subprocessor provides a level of security and privacy appropriate to their access to data and the scope of the services they are engaged to provide." URL: https://services.google.com/fh/files/misc/safeguards_for_international_data_transfers_with_google_cloud.pdf. Google describes in its public documentation (the list of sub-processors) that staff at the first category of sub-processors can only access Content Data if the customer gives permission, for example by granting access to a Google Drive folder with recorded Meets or transcripts. But the second category of Google subsidiaries can access Content Data without such clear consent, if authorized by Google and required. Google explains in its Security Overview (last updated May 2022) that security is central to its everyday operations and to disaster planning, including how we address threats. It's prioritized in the way we handle customer data, our account controls, our compliance audits, and our certifications. As part of the organisational measures Google offers results of audits through its Compliance reports manager. Though these reports or certificates are only accessible if the Additional Service Google Developers is activated (which should be disabled), Google has clarified that Dutch Education Workspace admins can request direct access to the SOC2 and BSI C5 audit reports through their account manager. According to a Google 2021 whitepaper on Safeguards for international data transfers with Google Cloud, Google offers Access Transparency to Workspace customers to review logs of actions for covered service data taken by Google staff when accessing certain customer data as permitted by law. Google also writes: "In line with our Trust Principles, we never give any government "backdoor" access." URL: https://services.google.com/fh/files/misc/safeguards_for_international_data_transfers_with_google_cloud.pdf. In reply to questions about access to encryption keys as part of 'backdoors', Google has further clarified: "Google will not disable security features or alter Meet systems to allow third parties to gain access to Customer Personal Data that would otherwise be unavailable to a third party in clear text." Google publishes separate transparency reports for compelled disclosure of data from Cloud and Workspace Education customers. URL: https://transparencyreport.google.com/user-data/enterprise?hl=en. Google describes its internal processes in its Government Requests for Cloud Customer Data whitepaper. Google has explained it has not provided any government with Meet Customer Data or Service Data belonging to an education institutions	Privacy Company has tested the effectivity of CSE for Meet with a self-controlled FlowCrypt key server, and third party (open source) identity provider, and encountered some issues. Currently, admins cannot centrally enforce the use of CSE for Meet, and the options for end users to enable CSE are hard to find. Google has announced a review of the interface, and will enable admins to centrally decide. However, Google is not willing to change the warning to end users that adding extra encryption prevents users from using the features recording, live streaming, connecting with a phone, use of breakout rooms, host management, polls, Q&A, noise cancellation, whiteboarding or transferring calls between Google Workspace apps. Another identified issue is the impossibility to invite guest users without Google account to use client-side encryption in a school-initiated Meet (for example, a parent teacher meeting about the progress of a pupil). Google explains in the article about CSE in Meet: The knocking capability to allow a guest is disabled. https://support.google.com/meet/answer/11605714?hl=en-GB). Finally, admins must once use the Google Cloud to create an API-key (to allow the external key server to talk to Google), a service that is outside the negotiated Workspace contract because Google Cloud is an Additional Service in Workspace. Google has assured that it is a processor for this limited use of the Google Cloud Platform in this case, based on the GCP Terms of Service (which incorporate the Google Cloud Processing Addendum).
k)	Relevant onward transfer(s) of personal data (if any):	Transient Content Data from Meet may be processed in all global data centres, but according to Google it is not possible for Google staff to join live meetings if they are not invited. Recorded Content Data from Meet is exclusively processed in the EU by Workspace for Education Plus, if they apply Data Regions. Even though this DTIA assumes that customers in practice will not apply CSE, customers with these (paid) licenses should use and apply CSE if they know their end users organise meetings in which sensitive or special categories of data are exchanged. The options for data region choice and CSE are not available for schools with the (free) Education Fundamentals licenses.	
l)	Countries of recipients of relevant onward transfer(s):	Australia, Brazil, Chile, Hong Kong, India, Singapore and Taiwan. Additionally, access may be obtained from the USA (no longer a third country). The potential (voluntary) transfer to support engineers in the 12 third countries in the context of a support request is out of scope. This DTIA assumes that Dutch public sector customers of Workspace will not provide consent for such access if they file a support ticket. However, their personal data may still be accessed in the 7 (other) third countries for technical support without their specific consent, if they file a support request. This latter type of processing is in scope of this DTIA.	Google has explained: "*If customers wish to avoid the possibility that a listed technical support Subprocessor could access Customer Data or Service Data for technical support purposes then* ***they are not required to use technical support****. Accordingly, customers may implement internal policies instructing their admins not to use Google's technical support services. They are, of course, also free to procure technical support from providers other than Google, such as their local Google Workspace reseller.*"

Step 2: Define the DTIA parameters

			Rationale
a)	Starting date of the transfer:	[assessment made on 28 November 2023]	
b)	Assessment period in years:	2	
c)	Ending date of the assessment based on the above:	X+2	
d)	Target jurisdiction for which the DTIA is made:	Australia, Brazil, Chile, Hong Kong, India, Singapore and Taiwan + United States	*This includes access for technical support by engineers in these 7 third countries. It is assumed that Dutch public sector Workspace customers will not consent to transfer of Content Data to the other list of subprocessors in 12 third countries in the context of a support request.*
e)	Is importer an Electronic Communications Service Provider as defined in	Yes	
f)	Does importer/processor commit to legally resist every request for access:	No	*Google explains in its "Government Requests for Cloud Customer Data" whitepaper that it commits to object to, or limit or modify, any legal process that it reasonably determines to be overbroad, disproportionate, incompatible with applicable law, or otherwise unlawful. See Step 2 on page 7.* *The confidential agreements with the Dutch Education customers include detailed commitments with regard to disclosure. Google has also explained in reply to this DTIA that it incidentally responds - voluntarily - to a request from a Third Country authority by disclosing very limited EEA personal data in emergency situations where it has a good faith belief that disclosure of EEA personal data to a Third Country government authority is necessary to prevent an imminent threat to life or serious physical injury. The Dutch Education sector does not agree that Google is entitled to such voluntary disclosures. Google has assured the Dutch education sector that it has not disclosed any personal data from Dutch Education customers in the past 2 years for this purpose.*
g)	Relevant local laws taken into consideration:	Google has not shared its legal analysis of applicable laws and their compliance with the fundamental right guarantees offered to data subjects in Australia, Brazil, Chile, Hong Kong, India, Singapore and Taiwan.	*This DTIA cannot provide a detailed legal analysis of the applicable surveillance laws in the 7 third countries. Absent such an analysis, it has to be assumed that some or all authorities in the third countries are permitted to obtain data from Google.* *Since the adequacy decision for the USA from the European Commission on 10 July 2023, transfers to the USA based on the DPF do not have to be complemented by supplementary measures. The Assessment has already been made by the European Commission, meaning that when the DPF applies, an additional assessment is not necessary. However, as controller the Dutch government still needs to assess the risks in all third final destination countries.*

Step 3: Probability that a foreign authority has a legal claim in the data and wishes to enforce it against the provider

		Probability	Cases	Cases remaining	Rationale
a)	Number of cases under the laws listed in Step 2g per year in which an authority in the third countries is estimated to attempt to obtain relevant data through legal action during the period under consideration.	100%	1,00		*In reply to this DTIA Google has stated it has not disclosed any Content Data from Dutch Education customers to law enforcement in the past two years: "We can confirm that, in the past two years (which we understand to be your 'assessment period'), we have not disclosed any Customer Data or Service Data belonging to public sector or education institutions located in the Netherlands in response to requests from law enforcement agencies (such as requests made under warrant or subpoena) based in Australia; Brazil; Chile; Hong Kong; India; Singapore; Taiwan; or the United States (US)." Google has also explicitly confirmed it has not voluntarily disclosed any personal data from Dutch Education customers in the past 2 years.* *Google does not provide information if EU Customer Content Data were disclosed to security services and intelligence agencies. Google only mentions a range between 0 and 499 at https://transparencyreport.google.com/user-data/us-national-security. For clarity, under US law, providers can neither confirm nor deny having received any specific legal demands subject to a secrecy obligation. It is plausible that the other third countries have similar secrecy obligations.* *Google is contractually committed to redirect orders for disclosure to its customers. If not possible, Google will evaluate if it is valid and binding order, If compelled to disclose personal data, Google will try to notify the customer and allow the customer to challenge the request, where legally permitted. URL: https://services.google.com/fh/files/blogs/government_access_technical_whitepaper.pdf* *Google's 'zero disclosure' to law enforcement authorities does not include orders from security services and intelligence agencies, which Google may not be permitted to redirect to its customers. The probability of such compelled disclosure cannot be set to zero. Absent more transparency about disclosure to security services and intelligence agencies the probability is set to 1 case per year*
b)	Share of such cases in which the request occurs in connection with a case that due to its nature in principle permits the authority to obtain the data also from a provider	100%	1,00		*Absent a detailed analysis of applicable laws in the 7 third countries, it has to be assumed that some or all authorities in the third countries are permitted to obtain data from Google. For example, as Hong Kong is part of China, governments across the EU have expressed concerns about access by Chinese authorities to personal data from EU citizens. As quoted above, though Google has not disclosed any Dutch Education customer data to law enforcement authorities in these countries in the past 2 years, disclosure to intelligence/security services or voluntary disclosure cannot be excluded.*
c)	Probability that in the remaining such cases it will be possible for the company to successfully cause the authority (by legal means or otherwise) to give up its request for the data **in plain text**	10%	0,90		*According to Google, CSE is not necessary for day-to-day use. Google explains: "This additional control can help you strengthen the confidentiality of your sensitive or regulated data. Your organization might need to use CSE for various reasons—for example:* *Privacy—Your organization works with extremely sensitive intellectual property.* *Regulatory compliance—Your organization operates in a highly regulated industry, like aerospace and defense, financial services, or government." URL: https://support.google.com/a/answer/10741897?sjid=5331145370927069105-EU.* *In view of the current complexity of CSE and Google's warnings to end users that many desired functionalities won't work, this DTIA assumes schools and universities will not apply CSE for day to day use. Therefore, the probability that Google is not able to produce the recorded data in clear text, is very low.*
d)	Probability that in the remaining cases the requested data will be provided in one way or another (e.g., with consent or through legal or administrative assistance)	1%	0,89		*Absent an MLAT with the third country, EU organisations cannot consent to disclose Content Data to a government authority in a third country, based on Art 48 GDPR. Google has explained in reply to this DTIA that it has not provided any personal data from Dutch Education customers to law enforcement authorities in the assessment period, also not on a voluntary basis.*
e)	Probability that in the remaining cases the authority will consider the data it is seeking to be so important that it will look for another way to obtain it	50%	0,45	0,45	*Enforcing lawful access via Google to access data of one of its Education customers (where it is a processor) is much more difficult than in the case of data of private individuals (where it is a controller). It also takes time. Therefore, we believe that the authorities will want to undergo such trouble only in particularly important cases, thus significantly reducing the number of relevant cases.*

Number of cases per year in which the question of lawful access by a foreign authority arises	0,45	Based on E35, which is a calculation of C35*D34. D34 is calculated as (1-C34)*D33
Number of cases in the period under consideration	0,89	Based on E37*C21

Step 4a: Probability that a foreign authority will successfully enforce the claim through the provider

Legal Basis considered for the following assessment: Unknown for Australia, Brazil, Chile, Hong Kong, India, Singapore and Taiwan, EU Adequacy Decision for registered participants in the EU-US Data Privacy Framework

Prerequisite for success		Probability per case			Rationale	
a)	Probability that the authority is aware of the provider and its subcontractors (prerequisite no. 1)	100%		100%	*Google is a well-known cloud services provider with a substantial amount of Workspace for Education Plus Customers in the EU*	
b)	Probability that an employee of the provider or its subcontractors will gain access to the data in plain text in a support-case ... (prerequisite no. 2)	0%	0,00%		*Google's employees in the 7 third countries are technically able to obtain access in plain text to recorded Content Data from Meet, as part of technical service maintenance and support, but they need to be authorised to access specific data [see below].* *Schools and universities can cannot prevent access to the recorded Content Data by the support engineers in these 7 third countries if they file a support request. They can only lower the probability of access for this purpose by never filing a support request with Google. However, that doesn't end the transfer. Google engineers in the 7 third countries may still have access to some Content Data for troubleshooting, releasing new code, making configuration changes or emergency maintenance purposes. Google has explained that customers can view the availability stats of Meet in the Netherlands to make an estimate of the probability of such transfers. These stats show an average uptime of 99.993 per cent. That means Meet is down for an average of 3 minutes per month, or, only available for 1 hour and 15 minutes in total during the last 2 years. This results in a probability of 0,007 per cent for access to the recorded Content Data.*	*Google has explained that the probability of access to specific content is very low, even absent CSE. "For context, the nature of Google Meet is such that the Customer Data that is 'generated' during a meeting is predominantly transient. For example, video and audio streams of a conversation between two Meet participants (e.g. a teacher and student). Google support agents would have no reason to join such a meeting as that would not be required for their role. Google Meet includes measures by default that prevent non-invitees from being able to join without explicit host admission. While recordings of Google Meet meetings (and other artifacts, like attendance reports, transcripts, etc) can be stored in Google Drive, Google support personnel would not be able to access that data unless the customer raised a support case and provided the agent with access to the Drive file(s)."*

	... and is able to search for, find and copy the data requested by the authority (prerequisite no. 3)	1%		0%	Google employees can incidentally be tasked to look at problems from Dutch customers with Meet, but they cannot 'search' for any customers' personal data. Google explains: "Access is entirely dependent on the specific activity they need to perform and only occurs where absolutely necessary to e.g. address the specific technical issue they are investigating." Google has taken many access control measures. Google explains: "An employee's authorization settings are used to control access to all resources, including Customer Data, Service Data and Google Meet systems. Even if an employee has the appropriate authorization to access Customer Data or Service Data, they must still provide a justification tied to a specific technical issue otherwise access to that data will be rejected. All technical issues are individually tracked using a unique case ID, and employee justifications are periodically reviewed. This means that it is not technically possible for an employee to access Customer Data or Service Data that is not required for them to investigate and resolve specific technical issues tasked to them. Access is monitored by our dedicated security teams as a check on the effectiveness of our controls. The security teams actively monitor access patterns and investigate unusual events." In reply to a question from Privacy Company about log controls, Google stated it has "not detected any unauthorised usage by engineers in the third countries in the past 2 years to a) Customer Data and b) Service Data." If Google obtains access to recorded Meet Content Data for technical support/maintenance, Google ensures that that access is limited to the data necessary to resolve the troubleshooting case and not more. Maintenance staff cannot simply search for other recorded data, while requests from authorities always refer to specific data. The probability that the Google subsidiary gets access to the specific data the government authority is looking for (for example, a recording of a meeting with a targeted end-user) is very low.
c)	Probability that despite the technical countermeasures taken, employees of the provider, of its subcontractors or of the parent company technically have access to data in plain text (also) outside a support situation (e.g., using admin privileges) or are able to gain such access, e.g., by covertly installing a backdoor or "hacking" into the system (irrespective of whether they are allowed to do so) ... (prerequisite no. 2)	10%	0,10%		This DTIA assumes schools and universities do not use CSE for day to day use. In the regular Meet, Google applies encryption to the data-at-rest, but Google has access to the key, and can therefore (theoretically) decrypt these data if ordered to do so. Though Google has not provided any personal data from Dutch Education customers to law enforcement in the past 2 years, Google is prohibited from publishing details about disclosure to security services. In reply to this DTIA Google has explained it has not built in any backdoors. "Google has not provided any government with direct access to any information stored in our data centers, including data stored or processed by the Meet application." Google has also stated: "Google has not joined any program that would give the U.S. government—or any other government—direct access to its servers." Google has clarified that this statement also applies to indirect access through for example, distribution of a new version or temporary lifting of transit encryption. "Google will not disable security features or alter Meet systems to allow third parties to gain access to Customer Personal Data that would otherwise be unavailable to a third party in clear text." In view of the strict access controls described in row 47 and the fact that Google has not detected any unauthorised usage by engineers in the past 2 years, the probability of access to the recorded data in plain text (without CSE) is estimated to be a maximum of 10%, based on the assumption that authorities in the third countries do have legal powers to compel Google to decrypt with its own keys, and to disclose these data.
	... and are then able to search for, find and copy the data requested by the	1%			It is unlikely that Google employees in these third countries would succeed in gaining access and be able to search for the data specifically
d)	Probability that the provider, the subcontractor or its parent company, respectively, is located within the jurisdiction of the authority (prerequisite no. 4)	100%		100%	Google explains in its information about subprocessors that its subsidiaries in the 7 third countries may have access to (recorded) Content Data from Meet for the purposes of software and systems engineering, maintenance and troubleshooting. See: https://workspace.google.com/terms/subprocessors.html.
e)	Probability that despite the technically limited access and the technical and organizational countermeasures in place, the authority is permitted to order the provider, its subcontractor or the parent company, respectively, to obtain access to the data and produce it to the authority in plain text (prerequisite no. 5)	50%		50%	Speculative estimate. This DTIA assumes schools and universities do not use CSE for day to day use. Though Google by default applies encryption to both streaming and recorded data, Google has access to these keys, can use these keys to decrypt if necessary for troubleshooting, and can hence also be ordered to decrypt the data. Therefore the probability that government authorities in the 3d countries can obtain access to the recorded data is high, but not 90%, as there won't be recorded data from all Meets (no recording or transcript made, or retention period expired), and hence, it is not certain that the Google subsidiary would find the data specifically requested by an authority.
f)	Probability that if data were to be handed over to the foreign authority, this would lead to the criminal liability of employees of the provider or its subcontractors, the prosecution of which would be possible and realistic, and as a consequence, the data does not have to be produced or is not produced (prerequisite no. 6)	50%		50%	Privacy Company has studied the confidential SOC-2 and C5:2020 audit reports. These reports do not note any deviations/findings with regard to transfers and disclosure of Content Data to third parties to fulfil requests. Additionally, Google has a Code of Conduct, in which it mentions the existence of anti-bribery laws, with the following sentence: "Like all businesses, Google is subject to lots of laws, both U.S. and non-U.S., that prohibit bribery in virtually every kind of commercial setting." URL: https://abc.xyz/investor/google-code-of-conduct/ All Google employees are required to follow this Code. The probability is set to 50% because the (existence of) anti bribery laws in the 7 third countries is unknown.
g)	Probability that the government or education organisation does not succeed in removing the relevant data in time or otherwise withdrawing it from the provider's access (prerequisite no. 7)	50%		50%	Google has explained it has not disclosed any Content Data belonging to public sector or education institutions located in the Netherlands in response to requests from law enforcement agencies (such as requests made under warrant or subpoena) based in Australia; Brazil; Chile; Hong Kong; India; Singapore; Taiwan; or the United States (US), nor voluntarily disclosed any data from Dutch government and education organisations in reply to requests from law enforcement in emergency situations in the past 2 years. However, Google is prohibited from publishing statistics about disclosure to security services/intelligence agencies. It is plausible that Google will be subjected to gagging order and not permitted to inform its Customer. Hence Google may not be in a position to issue a timely warning to its customer. If such an order is issued for a recorded Meet, the probability is set to 50%, assuming only 50% of Meets are recorded, and hence, available via Drive. Schools and universities can further lower this probability by not making any recordings of Meets or at least apply a very short retention period.

Residual risk of successful lawful access by a foreign authority through the provider (given the countermeasures): 0,01% Result of multiplication of E45*E46*E50*E51*E52*E53

Step 4b: Probability of foreign lawful access by mass surveillance of contents

Legal Basis considered for the following assessment: Unknown for Australia, Brazil, Chile, Hong Kong, India, Singapore and Taiwan, EU Adequacy Decision for registered participants in the EU-US Data Privacy Framework including FISA

		Probability in the period			**Rationale**
a)	Probability that the data at issue is transmitted to the provider or its subcontractors in a manner that permits the telecommunications providers in the country to view it in plain text as part of an upstream monitoring of Internet backbones	0%	0,00%	0,05%	This DTIA assumes schools and universities do not use CSE for day to day use. However, Google applies encryption in transit for inter-region data traffic and global routing (ALTS and TLS, plus the MTA-STS standard for mail), and AED for data stored at rest. Google also writes it never gives any government "backdoor" access." In reply to questions about access to encryption keys as part of 'backdoors', Google has further clarified: "Google will not disable security features or alter Meet systems to allow third parties to gain access to Customer Personal Data that would otherwise be unavailable to a third party in clear text."
b)	Probability that the data transmitted will include content picked by	0%			See the explanation in the row above.
c)	Probability that the provider or a subcontractor in the country is	10%	0,05%		As Google applies the encryption, Google and its subsidiaries are technically capable of lifting that encryption, and can do so in practice for
d)	Probability that the provider or a subcontractor in the countries above may be legally required to perform such as search (also) with the company's data	1%			Speculative estimate. This refers to Upstream Data Collection. According to the Adequacy Decision from the European Commission, personal data may be transferred to companies in the USA certified under the DPF without having to put additional supplementary measures (as described by the European Court of Justice and in the recommendations from the EDPB) in place. It is plausible that some Content Data from a Dutch government organisation or school/university are interesting for security services in the 7 third countries where they may be accessed. This probability is low based on Google's statement that it has **not provided any government with direct access to any information stored in its data centers, including data stored or processed by the Meet application (i.e. including direct access for security services).**
e)	Probability that the data is regarded as content that is the subject of intelligence searches in the country as per the above laws	50%			It is plausible that some Content Data from a Dutch education organisation are interesting for security services in the 7 third countries where they may be accessed. This DTIA assumes schools and universities will not deploy CSE for day to day use, and rely on the encryption applied by Google. Because the majority of Meets will not be encrypted, the probability of interest in the personal data in Content Data is estimated to be 50%.

Residual risk of successful lawful access by a foreign intelligence service without any guarantee of legal recourse (in view of the countermeasures): 0,05%

Step 5: Overall assessment

Probability that the question of lawful access via the cloud provider will arise at all (1 case in the period = 100%)	89,10%
Probability of successful lawful access by the foreign authorities concerned in these cases despite the countermeasures	0,01%
Probability of additional successful lawful access by a foreign intelligence service where there is no guarantee of legal recourse (despite	0,05%
Overall probability of a successful lawful access to data in plain text via the cloud provider in the observation period:	0,06%
Description in words (based on Hillson*):	Very low
The number of years it takes for a lawful access to occur at least once with a **90 percent** probability:	7.529
The number of years it takes for a lawful access to occur at least once with a **50 percent** probability:	2.267

... assuming that the probability neither increases nor decreases over time (like tossing a coin)

** Scale: <5% = "Very low", 5-10% = "Low", 11-25 = "Medium", 26-50% = "High" and >50% = "Very high" (by David Hillson, 2005, see https://www.pmi.org/learning/library/describing-probability-limitations-natural-language-7556).*

Step 6: Data subject risks

				Rationale
a)	*Estimated probability of occurrence of successful lawful access risk:*	*0,06%*	*Very Low*	
		4= special categories of data in the clear	*High*	*The recorded Content Data can include special categories of data. Even though the factual probability of unauthorised access is very low, the impact of such access to special categories of personal data in Content Data in plain text is high. Therefore, if schools and universities do not use CSE for Meets in which special categories of data are processed, this leads to a high risk. Though there are no high risks anymore for the transfer to the USA, such guarantees are not available for transfer to Google's data centres in Australia; Brazil; Chile; Hong Kong; India; Singapore and Taiwan.*
b)	*Estimated impact of risk*			

Very High	Low	High	High	High	High
High	Low	Medium	High	High	High
Medium	Low	Medium	Medium	High	High
Low	Low	Low	Medium	Medium	High
Very Low	Low	Low	Low	Low	High
	0	1	2	3	4

High

Step 7: Define the safeguards in place

				Rationale
a)	Would it be feasible, from a practical, technical and economical point of view, for the data exporter to transfer the personal data in question to a location in a whitelisted country instead?	Yes	*Describe why you still do not pursue this option*	*Google allows its Workspace for Education Plus to select datacentres in the EU to store the Content Data from Meet. See: Google, Data regions: Choose a geographic location for your data, URL: https://support.google.com/a/answer/7630496?hl=en. Google explains that the covered data in the data region policy include meet recordings, including chats (.SBV files), in Drive. Other covered data includes attendance reports, polling results, transcripts, questions, the submitter of question, and Jamboard. Google is "on schedule" with its publicly announced expansion of the data region choice paid Workspace customers with access controls to prevent access for support outside of the EU, processing-in-region along with an in-country copy by the end of 2023. See: https://workspace.google.com/blog/product-announcements/announcing-sovereign-controls-for-google-workspace. However, storage in the EU does not prevent technical engineers in the 7 third countries from accessing these data, when required and necessary. Google has not disclosed any plans to limit this access to EU-based engineers only. The data region choice also does not cover the transient data processing during the live conference calls. This means the streaming data can be processed by all global Google datacentres. Google has explained that there is no administrative access from Google to in-progress meetings, because non-invitees are prohibited from joining. See: https://workspace.google.com/blog/product-announcements/announcing-sovereign-controls-for-google-workspace.*
b)	Is the personal data transferred under one of the exemptions pursuant to applicable data protection law (e.g., Art. 49 GDPR in case of the GDPR)?	No		*Even though the probability of access by tech engineers in third countries to the data stored in the EU is very small, once an education organisation uses Google Meet the transfer is structural, not incidental.*
c)	Is the personal data at issue transmitted to the target jurisdiction in clear text (i.e. there is no appropriate encryption in-transit)?	No	*Ensure that data remains encrypted*	*No, Google by default applies encryption both in-transit and to stored data, but with its own keys. Customers can deploy CSE with their own key server, but Google does not recommend this for daily use. This DTIA assumes that schools and universities do not use CSE for day to day use.*
d)	Is the personal data at issue accessible in the target jurisdiction in clear text by the data importer/recipient or a third party (i.e. the data is either not appropriately encrypted or access to the keys to decrypt is possible)?	Yes	*Foreign lawful access is at least technically possible*	*As explained in row 96 above, this DTIA assumes schools and universities do not use CSE for day to day use. Therefore, Google and its subsidiaries in third countries can technically access the unencrypted recordings/transcriptions of meetings, although this would be a violation of policy and organisational measures.*
e)	Is the personal data at issue protected by a transfer mechanism approved by the applicable data protection law (e.g., the EU Standard Contractual Clauses in case of the GDPR, approved BCR, or - in the case of an onward transfer - a back-to-back-contract in line with the EU SCCs), and can you expect compliance with it, insofar permitted by the target jurisdiction, and judicial enforcement (where applicable)?	Yes	*Ensure that the mechanism remains in place and is complied with*	*The Dutch education customers rely on appropriate transfer mechanisms under Chapter V GDPR.*

Based on the answers given above, the transfer of sensitive and special categories of data without CSE is: **Not Permitted**

Final Step: Conclusion

In view of the above and the applicable data protection laws, the transfer of sensitive and special categories of data without CSE is:	**not permitted**
In view of the above and the applicable data protection laws, the transfer of regular personal data is:	**permitted**

This Transfer Impact Assessment has been made by:
SLM Rijk / SURF / SIVON / PRIVACY COMPANY

Place, Date:
Signed:
By: [School or University X]

Data Transfer Impact Assessment (DTIA) on the transfer to third countries of Account Data processed by Google Meet (audio/video conferencing)

Note: this tab describes the transfer of **Account Data**. For Google, Account Data are part of **Service Data**. See: https://cloud.google.com/terms/cloud-privacy-notice?hl=en. Google explains: "*Service Data consists of: Account information. We collect the data you or your organization provide when creating an account for Cloud Services or entering into a contract with us (username, names, contact details and job titles).* "
Because customers provide names themselves, it would be logical if Account Data were part of the Customer Data. Customers can limit the transfers of stored Content Data, but not of Account Data. Because there are differences in both the impact and the probability of unauthorised access to the different personal data, this DTIA continues to distinguish between 6 categories of personal data. This distinction also make this DTIA more comparable with other public DTIAs on videoconferencing services.

Step 1: Describe the intended transfer

			COMMENTS GOOGLE
a)	Data exporter (or the sender in case of a relevant onward transfer):	Dutch education and research organisation [X]	
b)	Country of data exporter:	**[Confidential]** for the Dutch education sector.	Technically, Google maintains servers around the world and its support and service engineers in the 7 third countries can access data anywhere, if necessary and authorised.
c)	Data importer (or the recipient in case of a relevant onward transfer):	Google LLC in the USA. The Dutch education customers rely on appropriate transfer mechanisms under Chapter V GDPR.	
d)	Country of data importer:	USA, with onward transfers to third countries for recorded data. The contracting entity for Dutch education customers of Google Workspace is **Google Cloud EMEA Limited** (see https://cloud.google.com/terms/google-entity), a Google entity based in Dublin, Ireland. Google Cloud EMEA Limited is a wholly owned subsidiary of Google LLC, which in turn is a wholly owned subsidiary of Alphabet Inc.	
e)	Context and purpose of the transfer:	Google Meet (https://apps.google.com/intl/en/meet/) provides the ability to organise and participate in video conferences, which can consist of 1-on-1 or group calls (up to 500 participants) with both audio and video or just audio. The video conference service also offers related features such as text chatting and file sharing among participants, (AI generated) live captions of speech, and (AI) translations of live captions. This tab is about the transfer of the Account Data. Account Data may be stored in or accessed from multiple third countries and the United States. In its Data Transfer policy Google writes: "We maintain servers around the world and your information may be processed on servers located outside of the country where you live." URL: https://policies.google.com/privacy/frameworks. In its subprocessor documentation, Google explains that there are two kinds of transfer: (1) for support and (2) (a) for data centre operations, (b) service maintenance and (c) technical support. 1. If a customer asks for support, and explicitly elects to enable access to Account Data in the course of a support case (e.g., by granting access to a Google Doc, Google Sheet, or Google Drive folder). In that case, the Account Data may be transferred to 12 third countries (without an adequacy decision from the EU): Australia, Brazil, Chile, El Salvador, Guatemala, Hong Kong, India, Malaysia, Mexico, Philippines, Singapore and Taiwan, plus the USA. 2. Google does not access any personal data for the first sub purpose of data centre operations. For the second and third sub purpose Google engineers in all locations have limited, authorized access to (recorded) Account Data for troubleshooting of all kinds of technical issues, releasing new code, making configuration changes or emergency maintenance purposes as well as mitigation of customer-initiated support requests. Google uses subprocessors in 7 third countries that may have access to the Content Data: Australia, Brazil, Chile, Hong Kong, India, Singapore and Taiwan. Additionally, access may be obtained from the USA. See https://workspace.google.com/terms/subprocessors.html for Google's public documentation. Google has provided confidential information relating to its subprocessors and affiliates to SURF and SIVON. Google has explained the probability of this transfer is very low: "Google service maintenance engineers located in Australia, Brazil, Chile, Hong Kong, India, Singapore, or Taiwan have not accessed any Google Meet Customer Data or Service Data belonging to public sector or education institutions located in the Netherlands in the past two years."	Google has not answered the question if Google Account Data from guest users in meetings organised by Education customers are offered the same processing guarantees. This DTIA assumes there is no such protection umbrella. Note Privacy Company: Google does not ask for specific consent for the transfer of Account Data (as part of Google's category Service Data) to employees in the first list of 12 third countries: the support employees only asks for consent to access to Content or Service Data of the customer without informing the customer in what country they operate. That is why this DTIA assumes that schools and universities will not provide such consent.
f)	Categories of data subjects concerned:	Google Workspace administrators, students and employee users of Dutch education and research organisations + external participants in Meet conferences (as guest users, or with a Google account).	
g)	Categories of personal data transferred:	E-mail, name and login/password combination from admins, employees and students used for Google Workspace to use Meet, and consumer Google Account Data from users participating as guests. A Google account is necessary if the school or government organisation has chosen the 'Trusted' or 'Restricted' setting (not the 'Open' access setting).	
h)	Sensitive and special categories of personal data:	Account Data from admins and employees can be sensitive, if their identity should remain confidential. The term sensitive data relates to the impact on data subjects if there is unauthorised access to their data. These data are different from the legal definition of special categories of data.	
i)	Technical implementation of the transfer:	**Google does not provide an option to any its Workspace customers (free or paid) to select datacentres in the EU to process the Workspace Account Data**, as the accounts are not mentioned on Google's limitative list of services for which a Data Region choice is available. See: Google, Data regions: Choose a geographic location for your data, URL: https://support.google.com/a/answer/7630496?hl=en. This DTIA assumes that Dutch public sector customers of Workspace won't provide consent for access by support engineers in the 12 third countries when they file a support request. As described in row 8, Google's subprocessors may access the Account Data in 7 third countries when this is necessary for service maintenance purposes and to respond to customer-initiated requests, even if a customer does not grant explicit consent for such access in relation to a support request.	
j)	Technical and organizational measures in place:	**Technical measures:** Google uses its own encryption in transit for inter-region data traffic and global routing (ALTS and TLS, plus the MTA-STS standard for mail), and AED for data stored at rest. Two technical measures available for Content Data are not available for Account Data: the additional protection of Access Approval to explicitly approve access to recordings and transcripts stored in Drive and the use of Client Side Encryption (CSE) for Meet. It follows from the technical investigation that the account name of the organiser is not just part of the Content Data (called 'Customer Data' by Google), but also part of the Diagnostic Data, as the directly identifiable Account Name of the organiser is leaked to Google as part of unencrypted Telemetry Data. Additionally, the Google accounts of guest users in meetings organised by a government organisation or educational institution are not covered by the additional data protection measures such as Sovereign Controls. **Organisational measures:** Google has provided contractual guarantees to the Dutch Education customers that sub-processors may only process personal data in accordance with the framework agreement, and that this guarantee applies to both the Content Data and the Diagnostic Data (Service Data). Google writes: "Before onboarding a subprocessor, Google conducts an audit of the security and privacy practices of the subprocessor to ensure the subprocessor provides a level of security and privacy appropriate to their access to data and the scope of the services they are engaged to provide." URL: https://services.google.com/fh/files/misc/safeguards_for_international_data_transfers_with_google_cloud.pdf. Google describes in its public documentation (the list of sub-processors) that staff at the first category of sub-processors can only access Content Data if the customer gives permission, for example by granting access to a Google Drive folder with recorded Meets or transcripts. But the second category of Google subsidiaries can access Account Data without such clear consent, if authorized by Google and required. Google explains in its Security Overview (last updated May 2022) that security is central to its "everyday operations and to disaster planning, including how we address threats. It's prioritized in the way we handle customer data, our account controls, our compliance audits, and our certifications." As part of the organisational measures Google offers results of audits through its Compliance reports manager. Though these reports or certificates are only accessible if the Additional Service Google Developers is activated (which should be disabled), Google has clarified that Dutch Workspace admins can request direct access to the SOC2 and BSI C5 audit reports through their account manager. According to a Google 2021 whitepaper on Safeguards for international data transfers with Google Cloud, Google offers Access Transparency to Workspace customers to review logs of actions for covered service data taken by Google staff when accessing certain customer data as permitted by law. Google also writes: "In line with our Trust Principles, we never give any government "backdoor" access." URL: https://services.google.com/fh/files/misc/safeguards_for_international_data_transfers_with_google_cloud.pdf. In reply to questions about access to encryption keys as part of 'backdoors', Google has further clarified: "Google will not disable security features or alter Meet systems to allow third parties to gain access to Customer Personal Data that would otherwise be unavailable to a third party in clear text." Google publishes separate transparency reports for compelled disclosure of data from Cloud and Workspace Education customers. URL: https://transparencyreport.google.com/user-data/enterprise?hl=en. Google describes its internal processes in its Government Requests for Cloud Customer Data whitepaper. Google has explained it has not provided any government with Meet Customer Data or Service Data belonging to a public sector or education	
k)	Relevant onward transfer(s) of personal data (if any):	<u>Account Data</u> from Meet may be transferred to 7 third countries for software and systems engineering, maintenance and troubleshooting, and for technical support.	
l)	Countries of recipients of relevant onward transfer(s):	Australia, Brazil, Chile, Hong Kong, India, Singapore and Taiwan. Additionally, access may be obtained from the USA (no longer a third country). If a customer agrees, support staff in 12 third countries may access the Account Data. This DTIA assumes that Dutch public sector customers of Workspace will not provide consent for such access if they file a support ticket. However, their Account Data may still be accessed in the 7 (other) third countries for technical support without their specific consent, if they file a support request. This latter type of processing is in scope of this DTIA.	

Step 2: Define the DTIA parameters

			Rationale
a)	Starting date of the transfer:	[assessment made on 28 November 2023]	
b)	Assessment period in years:	2	
c)	Ending date of the assessment based on the above:	X+2	
d)	Target jurisdiction for which the DTIA is made:	Australia, Brazil, Chile, Hong Kong, India, Singapore and Taiwan + United States	*This includes access for technical support by engineers in these 7 third countries. It is assumed that Dutch public sector Workspace customers will not consent to transfer of Account Data to the other list of subprocessors in 12 third countries in the context of a support request.*
e)	Is importer an Electronic Communications Service Provider as defined in	Yes	
f)	Does importer/processor commit to legally resist every request for access:	No	*Google explains in its "Government Requests for Cloud Customer Data" whitepaper that it commits to object to, or limit or modify, any legal process that it reasonably determines to be overbroad, disproportionate, incompatible with applicable law, or otherwise unlawful. See Step 2 on page 7.* *The confidential agreements with the Dutch Education customers include detailed commitments with regard to disclosure. Google has also explained in reply to this DTIA that it incidentally responds - voluntarily - to a request from a Third Country authority by disclosing very limited EEA personal data in emergency situations where it has a good faith belief that disclosure of EEA personal data to a Third Country government authority is necessary to prevent an imminent threat to life or serious physical injury. The Dutch Education sector does not agree that Google is entitled to such voluntary disclosures. Google has assured the Dutch education sector that it has not disclosed any personal data from Dutch Education customers in the past 2 years for this purpose.*
g)	Relevant local laws taken into consideration:	Google has not shared its legal analysis of applicable laws and their compliance with the fundamental right guarantees offered to data subjects in Australia, Brasil, Chile, Hong Kong, India, Singapore and Taiwan.	*This DTIA cannot provide a detailed legal analysis of the applicable surveillance laws in the 7 third countries. Absent such an analysis, it has to be assumed that some or all authorities in the third countries are permitted to obtain data from Google.* *Since the adequacy decision for the USA from the European Commission on 10 July 2023, transfers to the USA based on the DPF do not have to be complemented by supplementary measures. The Assessment has already been made by the European Commission, meaning that when the DPF applies, an additional assessment is not necessary. However, as controller the Dutch government still needs to assess the risks in all third final destination countries.*

Step 3: Probability that a foreign authority has a legal claim in the data and wishes to enforce it against the provider

		Probability	Cases	Cases remaining	Rationale
a)	Number of cases under the laws listed in Step 2g per year in which an authority in the third countries is estimated to attempt to obtain relevant data through <u>legal action</u> during the period under consideration.	100%	1,00		*In reply to this DTIA Google has stated it has not disclosed any Account Data (part of Google's category of Customer Data) from Dutch Education customers to law enforcement in the past two years: "We can confirm that, in the past two years (which we understand to be your 'assessment period'), we have not disclosed any Customer Data or Service Data belonging to public sector or education institutions located in the Netherlands in response to requests from law enforcement agencies (such as requests made under warrant or subpoena) based in Australia; Brazil; Chile; Hong Kong; India; Singapore; Taiwan; or the United States (US)." Google has also explicitly confirmed it has not voluntarily disclosed any personal data from Dutch Education customers in the past 2 years.* *Google does not provide information if EU Customer Account Data were disclosed to security services and intelligence agencies. Google only mentions a range between 0 and 499 at https://transparencyreport.google.com/user-data/us-national-security. For clarity, under US law, providers can neither confirm nor deny having received any specific legal demands subject to a secrecy obligation. It is plausible that the other third countries have similar secrecy obligations.* *Google is contractually committed to redirect orders for disclosure to its customers. If not possible, Google will evaluate if it is valid and binding order, If compelled to disclose personal data, Google will try to notify the customer and allow the customer to challenge the request, where legally permitted. URL: https://services.google.com/fh/files/blogs/government_access_technical_whitepaper.pdf* *The probability of such compelled disclosure cannot be set to zero. Absent more transparency about disclosure to security services and intelligence agencies the probability is set to 1 case per year.*
b)	Share of such cases in which the request occurs in connection with a case that due to its nature in principle permits the authority to obtain the data also from a provider	100%	1,00		*Absent a detailed analysis of applicable laws in the 7 third countries, it has to be assumed that some or all authorities in the third countries are permitted to obtain data from Google. For example, as Hong Kong is part of China, governments across the EU have recently expressed concerns about access by Chinese authorities to personal data from EU citizens. As quoted above, though Google has not disclosed any Dutch Education Account Data to law enforcement authorities in these countries in the past 2 years, disclosure to intelligence/security services or voluntary disclosure cannot be excluded.*
c)	Probability that in the remaining such cases it will be possible for the company to successfully cause the authority (by legal means or otherwise)	0%	1,00		*CSE is not available for Account Data. Therefore, the probability that Google is* ***not*** *able to produce the Account Data in clear text, is zero.*
d)	Probability that in the remaining cases the requested data will be provided in one way or another (e.g., with consent or through legal or administrative assistance)	1%	0,99		*Absent an MLAT with the third country, EU organisations cannot consent to disclose Account Data to a government authority in a third country, based on Art 48 GDPR. Google has explained in reply to this DTIA that it has not provided any personal data from Dutch Education customers to law enforcement authorities in the assessment period, also not on a voluntary basis.*
e)	Probability that in the remaining cases the authority will consider the data it is seeking to be so important that it will look for another way to obtain it	50%	0,50	0,50	*Enforcing lawful access via Google to access Account Data of one of its Education customers (where it is a processor) is much more difficult than in the case of data of private individuals (where it is a controller). It also takes time. Therefore, we believe that the authorities will want to undergo such trouble only in particularly important cases, thus significantly reducing the number of relevant cases.*
	Number of cases per year in which the question of lawful access by a foreign authority arises			0,50	Based on E35, which is a calculation of C35*D34. D34 is calculated as (1-C34)*D33
	Number of cases in the period under consideration			0,99	Based on E37*C21

Step 4a: Probability that a foreign authority will successfully enforce the claim through the provider

Legal Basis considered for the following assessment: Unknown for Australia, Brazil, Chile, Hong Kong, India, Singapore and Taiwan, EU Adequacy Decision for registered participants in the EU-US Data Privacy Framework

	Prerequisite for success	Probability per case			Rationale
a)	Probability that the authority is aware of the provider and its	100%		100%	*Google is a well-known cloud services provider with a substantial amount of Workspace for Education Plus Customers in the EU*
b)	Probability that an employee of the provider or its subcontractors will gain access to the data in plain text in a support-case ... (prerequisite no. 2)	0%	0,00%		*Google's employees in the 7 third countries are technically able to obtain access in plain text to Account Data used in Meet, as part of technical service maintenance and support, but they need to be authorised to access specific data [see below].* *Schools and universities can cannot prevent access to Account Data by the support engineers in these 7 third countries if they file a support request. They can only lower the probability of access for this purpose by never filing a support request with Google. However, that doesn't end the transfer. Google engineers in the 7 third countries may still have access to some Account Data for troubleshooting, releasing new code, making configuration changes or emergency maintenance purposes. Google has explained that customers can view the availability stats of Meet in the Netherlands to make an estimate of the probability of such transfers. These stats show an average uptime of 99.993 per cent. That means Meet is down for an average of 3 minutes per month, or, only available for 1 hour and 15 minutes in total during the last 2 years. This results in a probability of 0,007 per cent for access to the recorded Content Data.*
	... and is able to search for, find and copy the data requested by the authority (prerequisite no. 3)	1%		5%	*Google employees can incidentally be tasked to look at problems from Dutch customers with Meet, but they cannot 'search' for any customers' personal data. Google explains: "Access is entirely dependent on the specific activity they need to perform and only occurs where absolutely necessary to e.g. address the specific technical issue they are investigating." Google has taken many access control measures. Google explains: "An employee's authorization settings are used to control access to all resources, including Customer Data, Service Data and Google Meet systems. Even if an employee has the appropriate authorization to access Customer Data or Service Data, they must still provide a justification tied to a specific technical issue otherwise access to that data will be rejected. All technical issues are individually tracked using a unique case ID, and employee justifications are periodically reviewed. This means that it is not technically possible for an employee to access Customer Data [including the Account Data, comment added by Privacy Company] or Service Data that is not required for them to investigate and resolve specific technical issues tasked to them. Access is monitored by our dedicated security teams as a check on the effectiveness of our controls. The security teams actively monitor access patterns and investigate unusual events." In reply to a question from Privacy Company about log controls, Google stated it has "not detected any unauthorised usage by engineers in the third countries in the past 2 years to a) Customer Data and b) Service Data."*

c)	Probability that despite the technical countermeasures taken, employees of the provider, of its subcontractors or of the parent company technically have access to data in plain text (also) outside a support situation (e.g., using admin privileges) or are able to gain such access, e.g., by covertly installing a backdoor or "hacking" into the system (irrespective of whether they are allowed to do so) ... (prerequisite no. 2)	10%	5,00%		*CSE is not available for Account Data. Google applies encryption to the data-at-rest, but Google has access to the key, and can therefore (theoretically) decrypt these data if ordered to do so. Though Google has not provided any personal data from Dutch Education customers to law enforcement in the past 2 years, Google is prohibited from publishing details about disclosure to security services.* *In reply to this DTIA Google has explained it has not built in any backdoors. "Google has not provided any government with direct access to any information stored in our data centers, including data stored or processed by the Meet application." Google has also stated: "Google has not joined any program that would give the U.S. government—or any other government—direct access to its servers." Google has clarified that this statement also applies to indirect access through for example, distribution of a new version or temporary lifting of transit encryption. "Google will not disable security features or alter Meet systems to allow third parties to gain access to Customer Personal Data that would otherwise be unavailable to a third party in clear text." In view of the strict access controls described in row 47 and the fact that Google has not detected any unauthorised usage by engineers in the past 2 years, the probability of access to Account Data in plain text is estimated to be a maximum of 10%, based on the assumption that authorities in the third countries do have legal powers to compel Google to decrypt with its own keys, and to disclose these data.*
	... and are then able to search for, find and copy the data requested by the	50%			*It is not certain that Google employees in the USA and in the third countries would succeed in gaining access and be able to search for the*
d)	Probability that the provider, the subcontractor or its parent company,	100%		100%	*Google explains in its information about subprocessors that its subsidiaries in 7 third countries may have access to Account Data (as part of*
e)	Probability that despite the technically limited access and the technical and organizational countermeasures in place, the authority is permitted to order the provider, its subcontractor or the parent company, respectively, to obtain access to the data and produce it to the authority in plain text	100%		100%	*Speculative estimate. Though Google by default applies encryption to data-at-rest, including Account Data, Google has access to these keys, can use these keys to decrypt if necessary for troubleshooting, and can hence also be ordered to decrypt the data. Therefore the probability that government authorities in the third countries can order Google to provide access to the Account Data is set to 100%. [Note: the difference with Content Data is that no all Meets are recorded, and only retained for a short period of time].*
f)	Probability that if data were to be handed over to the foreign authority, this would lead to the criminal liability of employees of the provider or its subcontractors, the prosecution of which would be possible and realistic, and as a consequence, the data does not have to be produced or is not produced (prerequisite no. 6)	50%		50%	*Privacy Company has studied the confidential SOC-2 and C5:2020 audit reports. These reports do not note any deviations/findings with regard to transfers and disclosure of Content Data (including the Account Data) to third parties to fulfil requests. The audit reports do not cover the usage of Diagnostic Data, and Account Data are also registered in telemetry data and in the audit logs. Google has a Code of Conduct, in which it mentions the existence of anti-bribery laws, with the following sentence: "Like all businesses, Google is subject to lots of laws, both U.S. and non-U.S., that prohibit bribery in virtually every kind of commercial setting." URL: https://abc.xyz/investor/google-code-of-conduct/ All Google employees are required to follow this Code. The probability is set to 50% because the (existence of) anti bribery laws in the 7 third countries is unknown.*
g)	Probability that the government organisation does not succeed in removing the relevant data in time or otherwise withdrawing it from the provider's access (prerequisite no. 7)	100%		100%	*Google has explained it has not disclosed any Account Data belonging to public sector or education institutions located in the Netherlands in response to requests from law enforcement agencies (such as requests made under warrant or subpoena) based in Australia; Brazil; Chile; Hong Kong; India; Singapore; Taiwan; or the United States (US), nor voluntarily disclosed any data from Dutch government and education organisations in reply to requests from law enforcement in emergency situations in the past 2 years. However, Google does not disclose statistics about disclosure to security services/intelligence agencies. It is plausible that Google will be subjected to gagging orders from security services, and not permitted to inform its Customer. Hence Google may not be in a position to issue a timely warning to its customer. The probability is set to 100% absent an explanation from Google.*

Residual risk of successful lawful access by a foreign authority through the provider (given the countermeasures): 2,50% Result of multiplication of E45*E46*E50*E51*E52*E53

Step 4b: Probability of foreign lawful access by mass surveillance of contents

Legal Basis considered for the following assessment: Unknown for Australia, Brazil, Chile, Hong Kong, India, Singapore and Taiwan, EU Adequacy Decision for registered participants in the EU-US Data Privacy Framework including FISA

		Probability in the period			Rationale
a)	Probability that the data at issue is transmitted to the provider or its subcontractors in a manner that permits the telecommunications providers in the country to view it in plain text as part of an upstream monitoring of Internet backbones	0%	0,00%	0,05%	*Google applies encryption in transit for inter-region data traffic and global routing (ALTS and TLS, plus the MTA-STS standard for mail), and AED for data stored at rest. Google also writes it never gives any government "backdoor" access." In reply to questions about access to encryption keys as part of 'backdoors', Google has further clarified: "Google will not disable security features or alter Meet systems to allow third parties to gain access to Customer Personal Data that would otherwise be unavailable to a third party in clear text."*
b)	Probability that the data transmitted will include content picked by	0%			*See the explanation in the row above.*
c)	Probability that the provider or a subcontractor in the country is	10%	0,05%		*As Google applies the encryption, Google and its subsidiaries are technically capable of lifting that encryption, and can do so in practice for*
d)	Probability that the provider or a subcontractor in the countries above may be legally required to perform such as search (also) with the company's data	1%			*Speculative estimate. This row refers to Upstream Data Collection. According to the Adequacy Decision from the European Commission, personal data may be transferred to companies in the USA certified under the DPF without having to put additional supplementary measures (as described by the European Court of Justice and in the recommendations from the EDPB) in place.* *It is plausible that some Account Data from a Dutch government organisation or school/university are interesting for security services in the 7 third countries where they may be accessed. This probability is low based on Google's statement that it has not provided any government with direct access to any information stored in its data centers, including data stored or processed by the Meet application (i.e. including direct access for security services).*
e)	Probability that the data is regarded as content that is the subject of intelligence searches in the country as per the above laws	50%			*It is plausible that some Account Data from a Dutch education organisation are interesting for security services in the 7 third countries where they may be accessed.schools and universities must rely on the encryption applied by Google. These data are more likely to be regarded as interesting information (as selectors) than the Content Data. Therefore the probability of interest in the personal data in Content Data is estimated to be 50%, and the probability of interest may even increase if security services deploy quantum computing to decrypt data.*

Residual risk of successful lawful access by a foreign intelligence service without any guarantee of legal recourse (in view of the countermeasures): 0,05%

Step 5: Overall assessment

Probability that the question of lawful access via the cloud provider will arise at all (1 case in the period = 100%)	99,00%
Probability of successful lawful access by the foreign authorities concerned in these cases despite the countermeasures	2,50%
Probability of additional successful lawful access by a foreign intelligence service where there is no guarantee of legal recourse (despite	0,05%
Overall probability of a successful lawful access to data in plain text via the cloud provider in the observation period:	2,53%
Description in words (based on Hillson*):	Very low
The number of years it takes for a lawful access to occur at least once with a **90 percent** probability:	180
The number of years it takes for a lawful access to occur at least once with a **50 percent** probability:	54

... assuming that the probability neither increases nor decreases over time (like tossing a coin)

** Scale: <5% = "Very low", 5-10% = "Low", 11-25 = "Medium", 26-50% = "High" and >50% = "Very high" (by David Hillson, 2005, see https://www.pmi.org/learning/library/describing-probability-limitations-natural-language-7556).*

Step 6: Data subject risks

				Rationale
a)	*Estimated probability of occurrence of successful lawful access risk:*	*2,53%* *3= regular personal data in the clear*	*Very Low* *High*	*Even though Account Data can include sensitive data, for this assessment it is assumed organisations will follow the recommendation to use pseudonyms for such specific employees and students. Hence, the Account Data are regular personal data. The impact of the risk of access to these personal data can be high, but the probability is very low. Therefore, the risk is low. Though there are no high risks anymore for the transfer to the USA, such guarantees are not available for transfer to Google's data centres in Australia; Brazil; Chile; Hong Kong; India; Singapore and Taiwan.*
b)	*Estimated impact of risk*			

Very High	Low	High	High	High	High
High	Low	Medium	High	High	High
Medium	Low	Medium	Medium	High	High
Low	Low	Low	Medium	Medium	High
Very Low	Low	Low	Low	Low	High
	0	1	2	3	4

Low

Step 7: Define the safeguards in place

				Rationale
a)	Would it be feasible, from a practical, technical and economical point of view, for the data exporter to transfer the personal data in question to a location in a whitelisted country instead?	Yes	*Describe why you still do not pursue this option*	*Google does not make a Data Region choice available for Account Data, not as part of the Content Data, and not as part of the Service Data. Google has not disclosed any plans to limit this access to EU-based engineers only. This means the Account Data can be processed by support engineers in the USA, and in the 7 third countries.*
b)	Is the personal data transferred under one of the exemptions pursuant to applicable data protection law (e.g., Art. 49 GDPR in case of the GDPR)?	No		*Even though the probability of access by tech engineers in third countries to the Account Data is very small, once an education organisation uses Google Meet the transfer is structural, not incidental.*
c)	Is the personal data at issue transmitted to the target jurisdiction in clear text (i.e. there is no appropriate encryption in-transit)?	No	*Ensure that data remains encrypted*	*No, Google by default applies encryption both in-transit and to stored data, but with its own keys. It is not possible to apply CSE to the Account Data.*
d)	Is the personal data at issue accessible in the target jurisdiction in clear text by the data importer/recipient or a third party (i.e. the data is either not appropriately encrypted or access to the keys to decrypt is possible)?	Yes	*Foreign lawful access is at least technically possible*	*Yes, Google and its subsidiaries in 3d countries can technically access the unencrypted Account Data, although this would be a violation of policy and organisational measures*
e)	Is the personal data at issue protected by a transfer mechanism approved by the applicable data protection law (e.g., the EU Standard Contractual Clauses in case of the GDPR, approved BCR, or - in the case of an onward transfer - a back-to-back-contract in line with the EU SCCs), and can you expect compliance with it, insofar permitted by the target jurisdiction, and judicial enforcement (where applicable)?	Yes	*Ensure that the mechanism remains in place and is complied with*	*The Dutch education customers rely on appropriate transfer mechanisms under Chapter V GDPR.*

Based on the answers given above, the transfer is: **permitted**

Final Step: Conclusion

In view of the above and the applicable data protection laws, the transfer is: **permitted**

Reassess at the latest by: X+2
(or if there are any changes in circumstances)

This Transfer Impact Assessment has been made by:
SLM Rijk / SURF / SIVON / PRIVACY COMPANY

Place, Date:
Signed: ______________________
By: [School or University X]

Data Transfer Impact Assessment (DTIA) on the transfer to third countries of Support Data processed by Google Meet (audio/video conferencing)

This tab describes the transfers of **Support Data**. Google considers the information about support requests a subsection of **Service Data.** This DTIA distinguishes between 5 categories of Service Data: data about support tickets, Account Data, Diagnostic Data, Security Data and Website Data. Support Data also include the contents of support tickets: even though for Google these data are part of the category of **Customer Data**, described in this DTIA as Content Data. Because there are differences in both the impact and the probability of unauthorised access to Support Data, this DTIA continues to distinguish between 6 categories of personal data. This distinction also make this DTIA more comparable with other public DTIAs on videoconferencing services.

Step 1: Describe the intended transfer

			COMMENTS GOOGLE
a)	Data exporter (or the sender in case of a relevant onward transfer):	Dutch education and research organisation [X]	
b)	Country of data exporter:	**[Confidential]** for the Dutch education sector.	Technically, Google maintains servers around the world and its support and service engineers in the 7 third countries can access data anywhere, if necessary and authorised.
c)	Data importer (or the recipient in case of a relevant onward transfer):	Google LLC in the USA. The Dutch education customers rely on appropriate transfer mechanisms under Chapter V GDPR.	
d)	Country of data importer:	USA, with onward transfers to third countries for recorded data. The contracting entity for Dutch education customers of Google Workspace is **Google Cloud EMEA Limited** (see https://cloud.google.com/terms/google-entity), a Google entity based in Dublin, Ireland. Google Cloud EMEA Limited is a wholly owned subsidiary of Google LLC, which in turn is a wholly owned subsidiary of Alphabet Inc.	
e)	Context and purpose of the transfer:	Google Meet (https://apps.google.com/intl/en/meet/) provides the ability to organise and participate in video conferences, which can consist of 1-on-1 or group calls (up to 500 participants) with both audio and video or just audio. The video conference service also offers related features such as text chatting and file sharing among participants, (AI generated) live captions of speech, and (AI) translations of live captions. This tab is about the access to support tickets by google engineers in third countries, including attachments sent by customers. Support tickets may be stored in or accessed from multiple third countries and the United States. In its Data Transfer policy Google writes: "We maintain servers around the world and your information may be processed on servers located outside of the country where you live." URL: https://policies.google.com/privacy/frameworks. Google allows its Workspace Education customers to select datacentres in the EU to process the Content Data from Meet, but such a data region choice is not available for the data Google calls 'Service Data'. This category includes the Support Data. Google has clarified in reply to this DTIA: "personal data processed via Google Workspace is either Service Data or Customer Data - it cannot be both. For the sake of providing a response, we assume you intend "Support Data" to refer to e.g. information provided by customers in support tickets when requesting TSS, including attachments. We would categorise this as "Service Data". Google has clarified that sub-processors and subsidiaries that are given access to Content Data (Customer Data) also have access to Service Data. In its subprocessor documentation, Google explains that there are two kinds of transfer: (1) for support and (2) (a) for data centre operations, (b) service maintenance and (c) technical support. 1. If a customer asks for support, and explicitly elects to enable access to Support Data in the course of a support case (e.g., by granting access to the personal data necessary to reproduce or mitigate a problem). In that case, the Account Data may be transferred to 12 third countries (without an adequacy decision from the EU): Australia, Brazil, Chile, El Salvador, Guatemala, Hong Kong, India, Malaysia, Mexico, Philippines, Singapore and Taiwan, plus the USA. This DTIA assumes that Dutch public sector customers do not give such consent. Therefore transfer to the first list of subprocessors is out of scope. 2. However, even if a customer does not consent to transfer personal data to solve a support ticket, Google engineers may still have limited, authorized access to Support Data for infrastructure maintenance and troubleshooting all kinds of technical issues, and to remediate customer-initiated support requests. Google uses subprocessors in 7 third countries that may have access to the Support Data: Australia, Brazil, Chile, Hong Kong, India, Singapore and Taiwan. Additionally, access may be obtained from the USA. See https://workspace.google.com/terms/subprocessors.html for Google's public documentation. Google has provided confidential information relating to its subprocessors and affiliates to SURF and SIVON. Google has explained the probability of this transfer is very low: "Google service maintenance engineers located in Australia, Brazil, Chile, Hong Kong, India, Singapore, or Taiwan have not accessed any Google Meet Customer	Note Privacy Company: Google does not ask for specific consent for the transfer of Content Data to employees in the first list of 12 third countries: the support employees only asks for consent to access to Content or Service Data of the customer without informing the customer in what country they operate. **That is why this DTIA assumes that schools and universities will not provide such consent.**
f)	Categories of data subjects concerned:	Google Workspace administrators, students and employee users of Dutch education and research organisations + external participants in Meet conferences (as guest users, or with a Google account).	
g)	Categories of personal data transferred:	Support Data may include Account, Diagnostic and (snippets of) Content Data. As quoted above, in row 8, even though attachments sent by customers with support requests can include Content Data, if a customer for example would attach a crash log or a screenshot of a chat conversation, Google processes all Support Data as Service Data. This DTIA assumes schools and universities will follow the recommendation from the DPIA not to upload any sensitive data as part of a support ticket.	
h)	Sensitive and special categories of personal data:	Support Data may include Account Data from admins and employees whose identity should remain confidential, and snippets of Content Data from confidential Meets. The term sensitive data relates to the impact on data subjects if there is unauthorised access to their data. These data are different from the legal definition of special categories of data. This DTIA assumes schools and universities will follow the recommendation from the DPIA to pseudonymise account names of specific employees and students that incur high risks if their Account Data are accessed unlawfully.	
i)	Technical implementation of the transfer:	Google does not offer an option to Workspace Education customers to only allow support from EU based employees. Google has confirmed: "For clarity - and in case there has been any misunderstanding - we do not and are not legally required to), as part of a support case, seek a customer's 'consent' for transfers of Customer Data or Service Data to third countries for technical support purposes; nor do we offer controls that enable customers to 'toggle' whether their support case is handled from a third country or not." Therefore, this DTIA assumes Dutch schools and universities will not voluntarily consent to transfer to the Support Data to a support desk in one of the 12 third countries. However, as described in row 8, Google's subprocessors may access Support Data in 7 third countries when this is necessary for maintenance purposes, even if a customer does not grant explicit consent for such access in relation to a support request. Google is "on schedule" with its publicly announced expansion of the data region choice for Workspace for Education Plus customers with access controls to prevent access for support outside of the EU, and processing-in-region along with an in-country copy by the end of 2023. See: https://workspace.google.com/blog/product-announcements/announcing-sovereign-controls-for-google-workspace.	
j)	Technical and organizational measures in place:	Technical measures: Google applies its own encryption in transit for inter-region data traffic and global routing (ALTS and TLS, plus the MTA-STS standard for mail), and AED for data stored at rest. Google shows a pop-up to admins when they request technical support via the Admin Console, before submission, asking them to *"ensure you remove any sensitive data such as:* ●*Account passwords* ●*Cardholder data* ●*Confidential business data* ●*Personal health information* Google also warns against providing sensitive government information such as identification numbers or criminal justice information. Client Side Encryption (CSE) is not available for Support Data, as they are classified as 'Service Data' by Google. Organisational measures: Same as Content and Account Data	
k)	Relevant onward transfer(s) of personal data (if any):	Support Data from Meet may be transferred to 7 third countries for software and systems engineering, maintenance and troubleshooting, and for technical support. Only if a customer agrees, support staff in 12 third countries may access the Support Data. This DTIA assumes that Dutch public sector customers of Workspace will not give permission for such access if it involves transfer to 3d countries.	
l)	Countries of recipients of relevant onward transfer(s):	Australia, Brazil, Chile, Hong Kong, India, Singapore and Taiwan. Additionally, access may be obtained from the USA (no longer a third country)	Google has explained: "*If customers wish to avoid the possibility that a listed technical support Subprocessor could access Customer Data or Service Data for technical support purposes then they are not required to use technical support. Accordingly, customers may implement internal policies instructing their admins not to use Google's technical support services. They are, of course, also free to procure technical support from providers other than Google, such as their local Google Workspace reseller.*"

Step 2: Define the DTIA parameters

			Rationale
a)	Starting date of the transfer:	[assessment made on 28 November 2023]	
b)	Assessment period in years:	2	
c)	Ending date of the assessment based on the above:	X+2	
d)	Target jurisdiction for which the DTIA is made:	Australia, Brazil, Chile, Hong Kong, India, Singapore and Taiwan + United States	*This includes access for technical support by engineers in these 7 third countries. It is assumed that Dutch public sector Workspace customers will not consent to transfer of Account Data to the other list of subprocessors in 12 third countries in the context of a support request.*
e)	Is importer an Electronic Communications Service Provider as defined in	Yes	
f)	Does importer/processor commit to legally resist every request for access:	No	*Google explains in its "Government Requests for Cloud Customer Data" whitepaper that it commits to object to, or limit or modify, any legal process that it reasonably determines to be overbroad, disproportionate, incompatible with applicable law, or otherwise unlawful. See Step 2 on page 7.* *The confidential agreements with the Dutch Education customers include detailed commitments with regard to disclosure. Google has also explained in reply to this DTIA that it incidentally responds - voluntarily - to a request from a Third Country authority by disclosing very limited EEA personal data in emergency situations where it has a good faith belief that disclosure of EEA personal data to a Third Country government authority is necessary to prevent an imminent threat to life or serious physical injury. The Dutch Education sector does not agree that Google is entitled to such voluntary disclosures. Google has assured the Dutch educatio n sector that it has not disclosed any personal data from Dutch Education customers in the past 2 years for this purpose.*
g)	Relevant local laws taken into consideration:	Google has not shared its legal analysis of applicable laws and their compliance with the fundamental right guarantees offered to data subjects in Australia, Brasil, Chile, Hong Kong, India, Singapore and Taiwan.	*This DTIA cannot provide a detailed legal analysis of the applicable surveillance laws in the 7 third countries. Absent such an analysis, it has to be assumed that some or all authorities in the third countries are permitted to obtain data from Google.* *Since the adequacy decision for the USA from the European Commission on 10 July 2023, transfers to the USA based on the DPF do not have to be complemented by supplementary measures. The Assessment has already been made by the European Commission, meaning that when the DPF applies, an additional assessment is not necessary. However, as controller the Dutch government still needs to assess the risks in all third final destination countries.*

Step 3: Probability that a foreign authority has a legal claim in the data and wishes to enforce it against the provider

		Probability	Cases	Cases remaining	Rationale
a)	Number of cases under the laws listed in Step 2g per year in which an authority in the third countries is estimated to attempt to obtain relevant data through legal action during the period under consideration.	100%	1,00		*In reply to this DTIA Google has stated it has not disclosed any Support Data (as part of Service Data) from Dutch Education customers to law enforcement in the past two years: "We can confirm that, in the past two years (which we understand to be your 'assessment period'), we have not disclosed any Customer Data or Service Data belonging to public sector or education institutions located in the Netherlands in response to requests from law enforcement agencies (such as requests made under warrant or subpoena) based in Australia; Brazil; Chile; Hong Kong; India; Singapore; Taiwan; or the United States (US)." Google has also explicitly confirmed it has not voluntarily disclosed any personal data from Dutch Education customers in the past 2 years.* *Google does not provide information if EU Customer Support Data were disclosed to security services and intelligence agencies. Google only mentions a range between 0 and 499 at https://transparencyreport.google.com/user-data/us-national-security. For clarity, under US law, providers can neither confirm nor deny having received any specific legal demands subject to a secrecy obligation. It is plausible that the other third countries have similar secrecy obligations.* *Google is contractually committed to redirect orders for disclosure to its customers. If not possible, Google will evaluate if it is valid and binding order, If compelled to disclose personal data, Google will try to notify the customer and allow the customer to challenge the request, where legally permitted. URL: https://services.google.com/fh/files/blogs/government_access_technical_whitepaper.pdf* *The probability of such compelled disclosure cannot be set to zero. Absent more transparency about disclosure to security services and intelligence agencies the probability is set to 1 case per year.*
b)	Share of such cases in which the request occurs in connection with a case that due to its nature in principle permits the authority to obtain the data also from a provider	100%	1,00		*Absent a detailed analysis of applicable laws in the 7 third countries, it has to be assumed that some or all authorities in the third countries are permitted to obtain data from Google. For example, as Hong Kong is part of China, governments across the EU have expressed concerns about access by Chinese authorities to personal data from EU citizens. As quoted above, though Google has not disclosed any Dutch Education Support Data to law enforcement authorities in these countries in the past 2 years, disclosure to intelligence/security services cannot be excluded.*
c)	Probability that in the remaining such cases it will be possible for the company to successfully cause the authority (by legal means or otherwise) to give up its request for the data **in plain text**	0%	1,00		*CSE is not available for Support Data. Therefore, the probability that Google is not able to produce the Account Data in clear text, is zero.*
d)	Probability that in the remaining cases the requested data will be provided in one way or another (e.g., with consent or through legal or administrative assistance)	1%	0,99		*Absent an MLAT with the third country, EU organisations cannot consent to disclose Support Data to a government authority in a third country, based on Art 48 GDPR. Google has explained in reply to this DTIA that it has not provided any personal data from Dutch Education customers to law enforcement authorities in the assessment period, also not on a voluntary basis.*
e)	Probability that in the remaining cases the authority will consider the data it is seeking to be so important that it will look for another way to obtain it	10%	0,10	0,10	*Enforcing lawful access via Google to access Support data of one of its Education customers (where it is a processor) is much more difficult than in the case of data of private individuals (where it is a controller). As Support Data only cover limited datasets, the likelihood is much lower than requests for Content or Account Data. Therefore, we believe that the authorities will want to undergo such trouble only in particularly important cases, thus significantly reducing the number of relevant cases.*
	Number of cases per year in which the question of lawful access by a foreign authority arises			0,10	Based on E35, which is a calculation of C35*D34. D34 is calculated as (1-C34)*D33
	Number of cases in the period under consideration			0,20	Based on E37*C21

Step 4a: Probability that a foreign authority will successfully enforce the claim through the provider

Legal Basis considered for the following assessment: Unknown for Australia, Brazil, Chile, Hong Kong, India, Singapore and Taiwan, EU Adequacy Decision for registered participants in the EU-US Data Privacy Framework

Prerequisite for success		Probability per case			Rationale
a)	Probability that the authority is aware of the provider and its	100%		100%	*Google is a well-known cloud services provider with a substantial amount of Workspace for Education Plus Customers in the EU*
b)	Probability that an employee of the provider or its subcontractors will gain access to the data in plain text in a support-case ... (prerequisite no. 2)	0%	0,00%		*Customers can intentionally, with consent, allow Google support employees in 12 third countries to access Account Data in plain text as part of a support request. It is assumed that Dutch public sector Workspace customers will not consent to such a transfer. However, the Support Data can also be accessed without such consent by subprocessors in Australia, Brazil, Chile, Hong Kong, India, Singapore and Taiwan, as part of technical service maintenance and support, but they need to be authorised to access specific data [see below].* *Schools and universities can cannot prevent access to Support Data by the support engineers in these 7 third countries if they file a support request. They can only lower the probability of access for this purpose by never filing a support request with Google. However, that doesn't end the transfer. Google engineers in the 7 third countries may still have access to some personal data relevant for troubleshooting, releasing new code, making configuration changes or emergency maintenance purposes. Google has explained that customers can view the availability stats of Meet in the Netherlands to make an estimate of the probability of such transfers. These stats show an average uptime of 99.993 per cent. That means Meet is down for an average of 3 minutes per month, or, only available for 1 hour and 15 minutes in total during the last 2 years.*
	... and is able to search for, find and copy the data requested by the authority (prerequisite no. 3)	1%		1%	*Google employees can incidentally be tasked to look at problems from Dutch customers with Meet, but they cannot 'search' for any customers' personal data. Google explains: "Access is entirely dependent on the specific activity they need to perform and only occurs where absolutely necessary to e.g. address the specific technical issue they are investigating." Google has taken many access control measures. Google explains: "An employee's authorization settings are used to control access to all resources, including Customer Data, Service Data and Google Meet systems. Even if an employee has the appropriate authorization to access Customer Data or Service Data, they must still provide a justification tied to a specific technical issue otherwise access to that data will be rejected. All technical issues are individually tracked using a unique case ID, and employee justifications are periodically reviewed.* ***This means that it is not technically possible for an employee to access Customer Data or Service Data that is not required for them to investigate and resolve specific technical issues tasked to them.*** *Access is monitored by our dedicated security teams as a check on the effectiveness of our controls. The security teams actively monitor access patterns and investigate unusual events." In reply to a question from Privacy Company about log controls, Google stated it has "**not detected any unauthorised usage by engineers in the third countries in the past 2 years to a) Customer Data and b) Service Data.**"*

c)	Probability that despite the technical countermeasures taken, employees of the provider, of its subcontractors or of the parent company technically have access to data in plain text (also) outside a support situation (e.g., using admin privileges) or are able to gain such access, e.g., by covertly installing a backdoor or "hacking" into the system (irrespective of whether they are allowed to do so) ... (prerequisite no. 2)	10%	1,00%		*Though Google applies encryption to the data-at-rest, Google has access to the key, and can therefore (theoretically) decrypt these data if ordered to do so. Though Google has not provided any personal data from Dutch Education customers to law enforcement in the past 2 years, Google is prohibited from publishing details about disclosure to security services.* *In reply to this DTIA Google has explained it has not built in any backdoors. "Google has not provided any government with direct access to any information stored in our data centers, including data stored or processed by the Meet application." Google has also stated: "Google has not joined any program that would give the U.S. government—or any other government—direct access to its servers." Google has clarified that this statement also applies to indirect access through for example, distribution of a new version or temporary lifting of transit encryption. "Google will not disable security features or alter Meet systems to allow third parties to gain access to Customer Personal Data that would otherwise be unavailable to a third party in clear text." In view of the strict access controls described in row 47 and the fact that Google has not detected any unauthorised usage by engineers in the past 2 years, the probability of access to the Support Data in plain text is estimated to be a maximum of 10%, based on the assumption that authorities in the third countries do have legal powers to compel Google to decrypt with its own keys, and to disclose these data.*
	... and are then able to search for, find and copy the data requested by the	10%			*It is not plausible that Google would succeed in finding the data specifically requested by an authority in the Support Tickets (different from*
d)	Probability that the provider, the subcontractor or its parent company, respectively, is located within the jurisdiction of the authority (prerequisite no. 4)	100%		100%	*Google explains in its information about subprocessors that its subsidiaries in 7 third countries may have access to Support Data from Meet for the purposes of software and systems engineering, maintenance and troubleshooting, and for technical support. See: https://workspace.google.com/terms/subprocessors.html*
e)	Probability that despite the technically limited access and the technical and organizational countermeasures in place, the authority is permitted to order the provider, its subcontractor or the parent company, respectively, to obtain access to the data and produce it to the authority in plain text (prerequisite no. 5)	100%		100%	*Though Google by default applies encryption to data-at-rest, including Support Data, Google has access to these keys, can use these keys to decrypt if necessary for troubleshooting, and can hence also be ordered to decrypt the data. Therefore the probability that government authorities in the third countries can order Google to provide access to the Support Data is 100% (even if the chance that the requested data are available regarding a specific customer is very low).*
f)	Probability that if data were to be handed over to the foreign authority, this would lead to the criminal liability of employees of the provider or its subcontractors, the prosecution of which would be possible and realistic, and as a consequence, the data does not have to be produced or is not produced (prerequisite no. 6)	50%		50%	*Privacy Company has studied the confidential SOC-2 and C5:2020 audit reports. These reports do not note any deviations/findings with regard to transfers and disclosure of Content Data to third parties to fulfil requests. The audit reports do not cover the usage of Diagnostic Data, and Account Data are also registered in telemetry data and in the audit logs. Google has a Code of Conduct, in which it mentions the existence of anti-bribery laws, with the following sentence: "Like all businesses, Google is subject to lots of laws, both U.S. and non-U.S., that prohibit bribery in virtually every kind of commercial setting." URL: https://abc.xyz/investor/google-code-of-conduct/* *All Google employees are required to follow this Code. The probability is set to 50% because the (existence of) anti bribery laws in the 7 third countries is unknown.*
g)	Probability that the government organisation does not succeed in removing the relevant data in time or otherwise withdrawing it from the provider's access (prerequisite no. 7)	100%		100%	*Google has explained it has not disclosed any Support Data belonging to public sector or education institutions located in the Netherlands in response to requests from law enforcement agencies (such as requests made under warrant or subpoena) based in Australia; Brazil; Chile; Hong Kong; India; Singapore; Taiwan; or the United States (US), nor voluntarily disclosed any data from Dutch government and education organisations in reply to requests from law enforcement in emergency situations in the past 2 years. However, Google does not disclose statistics about disclosure to security services/intelligence agencies. It is plausible that Google will be subjected to gagging orders from security services, and not permitted to inform its Customer. Hence Google may not be in a position to issue a timely warning to its customer. The probability is set to 100% absent an explanation from Google.*

Residual risk of successful lawful access by a foreign authority through the provider (given the countermeasures): 0,50% Result of multiplication of E45*E46*E50*E51*E52*E53

Step 4b: Probability of foreign lawful access by mass surveillance of contents

Legal Basis considered for the following assessment: Unknown for Australia, Brazil, Chile, Hong Kong, India, Singapore and Taiwan, EU Adequacy Decision for registered participants in the EU-US Data Privacy Framework including FISA

		Probability in the period			Rationale
a)	Probability that the data at issue is transmitted to the provider or its subcontractors in a manner that permits the telecommunications providers in the country to view it in plain text as part of an upstream monitoring of Internet backbones	0%	0,00%	0,01%	*Google applies encryption in transit for inter-region data traffic and global routing (ALTS and TLS, plus the MTA-STS standard for mail), and AED for data stored at rest. Google also writes it never gives any government "backdoor" access." In reply to questions about access to encryption keys as part of 'backdoors', Google has further clarified: "Google will not disable security features or alter Meet systems to allow third parties to gain access to Customer Personal Data that would otherwise be unavailable to a third party in clear text."*
b)	Probability that the data transmitted will include content picked by	0%			*See the explanation in the row above.*
c)	Probability that the provider or a subcontractor in the country is	10%	0,01%		*As Google applies the encryption to the data-at-rest (in filed support tickets), Google and its subsidiaries are technically capable of lifting that*
d)	Probability that the provider or a subcontractor in the countries above may be legally required to perform such as search (also) with the company's data	1%			*Speculative estimate. This refers to Upstream Data Collection. According to the Adequacy Decision from the European Commission, personal data may be transferred to companies in the USA certified under the DPF without having to put additional supplementary measures (as described by the European Court of Justice and in the recommendations from the EDPB) in place.* *It is plausible that some Support Data from a Dutch government organisation or school/university are interesting for security services in the 7 third countries where they may be accessed. This probability is low based on Google's statement that* ***it has not provided any government with direct access to any information stored in its data centers, including data stored or processed by the Meet application*** *(i.e. including direct access for security services).*
e)	Probability that the data is regarded as content that is the subject of intelligence searches in the country as per the above laws	10%			*It is possible, but not likely that some Support Data from a Dutch education organisation are interesting for security services in the 7 third countries where they may be accessed. Since customers cannot encrypt Support Data with their own key, but the data are not as interesting as Content or Account Data, the probability of interest is set to 10%.*

Residual risk of successful lawful access by a foreign intelligence service without any guarantee of legal recourse (in view of the countermeasures): 0,01%

Step 5: Overall assessment

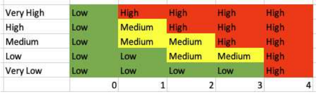
Probability that the question of lawful access via the cloud provider will arise at all (1 case in the period = 100%)	19,80%
Probability of successful lawful access by the foreign authorities concerned in these cases despite the countermeasures	0,50%
Probability of additional successful lawful access by a foreign intelligence service where there is no guarantee of legal recourse (despite	0,01%
Overall probability of a successful lawful access to data in plain text via the cloud provider in the observation period:	0,11%
Description in words (based on Hillson*):	Very low
The number of years it takes for a lawful access to occur at least once with a **90 percent** probability:	4.222
The number of years it takes for a lawful access to occur at least once with a **50 percent** probability:	1.271

... assuming that the probability neither increases nor decreases over time (like tossing a coin)

** Scale: <5% = "Very low", 5-10% = "Low", 11-25 = "Medium", 26-50% = "High" and >50% = "Very high" (by David Hillson, 2005, see https://www.pmi.org/learning/library/describing-probability-limitations-natural-language-7556).*

Step 6: Data subject risks

				Rationale
a)	*Estimated probability of occurrence of successful lawful access risk:*	*0,11%* *3= regular personal data in the clear*	*Very Low* *High*	*This assessment assumes Dutch public sector organisations will follow the advice from Google not to include any sensitive or special categories of data in attachments with support tickets. This assessment also assumes organisations will follow the recommendation to use pseudonyms for specific employees and students that incur high data protection risks if there is unauthorised access to their data. Hence, the Support Data should only contain regular personal data. The impact of unauthorised access to these personal data can be high, but the probability that the risk of unauthorised access occurs, is very low. Hence the risk is assessed as low.*
b)	*Estimated impact of risk*			



Very High	Low	High	High	High	High
High	Low	Medium	High	High	High
Medium	Low	Medium	Medium	High	High
Low	Low	Low	Medium	Medium	High
Very Low	Low	Low	Low	Low	High
	0	1	2	3	4

Low

Step 7: Define the safeguards in place

				Rationale
a)	Would it be feasible, from a practical, technical and economical point of view, for the data exporter to transfer the personal data in question to a location in a whitelisted country instead?	Yes	*Describe why you still do not pursue this option*	*Google does not make a Data Region choice available for Support Data, not as part of the Content Data, and not as part of the Service Data. Google has not disclosed any plans to limit this access to EU-based engineers only. This means the Support Data can be processed by support engineers in the USA, and in the 7 third countries.*
b)	Is the personal data transferred under one of the exemptions pursuant to applicable data protection law (e.g., Art. 49 GDPR in case of the GDPR)?	No		*Even though the probability of access by tech engineers in third countries to the Support Data, once an education organisation uses Google Meet the transfer is structural, not incidental.*
c)	Is the personal data at issue transmitted to the target jurisdiction in clear text (i.e. there is no appropriate encryption in-transit)?	No	*Ensure that data remains encrypted*	*No, Google by default applies encryption both in-transit and to stored data, but with its own keys. It is not possible to apply CSE to the Support Data.*
d)	Is the personal data at issue accessible in the target jurisdiction in clear text by the data importer/recipient or a third party (i.e. the data is either not appropriately encrypted or access to the keys to decrypt is possible)?	Yes	*Foreign lawful access is at least technically possible*	*Yes, Google and its subsidiaries in 3d countries can technically access the unencrypted Support Data, although this would be a violation of policy and organisational measures.*
e)	Is the personal data at issue protected by a transfer mechanism approved by the applicable data protection law (e.g., the EU Standard Contractual Clauses in case of the GDPR, approved BCR, or - in the case of an onward transfer - a back-to-back-contract in line with the EU SCCs), and can you expect compliance with it, insofar permitted by the target jurisdiction, and judicial enforcement (where applicable)?	Yes	*Ensure that the mechanism remains in place and is complied with*	*The Dutch education customers rely on appropriate transfer mechanisms under Chapter V GDPR.*

Based on the answers given above, the transfer is: permitted

Final Step: Conclusion

In view of the above and the applicable data protection laws, the transfer is: permitted

Reassess at the latest by: X+2

(or if there are any changes in circumstances)

This Transfer Impact Assessment has been made by:
SLM Rijk / SURF / SIVON / PRIVACY COMPANY

Place, Date:
Signed:
By: [School or University X]

Data Transfer Impact Assessment (DTIA) on the transfer to third countries of Diagnostic Data processed by Google Meet (audio/video conferencing)

This tab describes the transfers of **Diagnostic Data**. This category includes Telemetry Data from the end-user device and service generated server logs. Google considers Diagnostic Data a subsection of **Service Data**. This DTIA distinguishes between 5 categories of Service Data: data about support tickets, Account Data, Diagnostic Data, Security Data and Website Data. Because there are differences in both the impact and the probability of unauthorised access to these 4 categories, this DTIA continues to distinguish between 6 categories of personal data. This distinction also make this DTIA more comparable with other public DTIAs on videoconferencing services.

Step 1: Describe the intended transfer

			COMMENTS GOOGLE
a)	Data exporter (or the sender in case of a relevant onward transfer):	Dutch education and research organisation [X]	
b)	Country of data exporter:	**[Confidential]** for the Dutch education sector.	Technically, Google maintains servers around the world and its support and service engineers in the 7 third countries can access data anywhere, if necessary and authorised.
c)	Data importer (or the recipient in case of a relevant onward transfer):	Google LLC in the USA. The Dutch education customers rely on appropriate transfer mechanisms under Chapter V GDPR.	
d)	Country of data importer:	USA, with onward transfers to third countries for recorded data. The contracting entity for Dutch education customers of Google Workspace is **Google Cloud EMEA Limited** (see https://cloud.google.com/terms/google-entity), a Google entity based in Dublin, Ireland. Google Cloud EMEA Limited is a wholly owned subsidiary of Google LLC, which in turn is a wholly owned subsidiary of Alphabet Inc.	
e)	Context and purpose of the transfer:	Google Meet (https://apps.google.com/intl/en/meet/) provides the ability to organise and participate in video conferences, which can consist of 1-on-1 or group calls (up to 500 participants) with both audio and video or just audio. The video conference service also offers related features such as text chatting and file sharing among participants, (AI generated) live captions of speech, and (AI) translations of live captions. This tab is about the transfer of Diagnostic Data generated in Google service generated server logs, and in end-user generated Telemetry Data, including names of Meetings and the account name of the organiser of a Meet (as observed to be part of Telemetry Data). This tab does not include the specific webserver access logs maintained by Google with personal data about the access by guest users, end-users and admins to the login-page, the main entry page to participate in a Meet, and the Admin Console. This subset of Diagnostic Data is discussed in the separate tab Website Data. Service Data may be stored in or accessed from multiple third countries and the United States. In its Data Transfer policy Google writes: "We maintain servers around the world and your information may be processed on servers located outside of the country where you live." URL: https://policies.google.com/privacy/frameworks. Google allows its Workspace Education customers to select datacenters in the EU to process the Content Data from Meet, but such a data region choice is not available for the Diagnostic Data (which Google calls 'Service Data'). Google has clarified that sub-processors and subsidiaries that are given access to Content Data (Customer Data) also have access to Service Data. Therefore, the Diagnostic Data can be transferred in two circumstances: 1. If a customer explicitly elects to enable such access to for example audit logs or a crash log to help a Google support engineer solve the issue. In that case, the Diagnostic Data may be transferred to 12 third countries (without an adequacy decision from the EU): Australia, Brazil, Chile, El Salvador, Guatemala, Hong Kong, India, Malaysia, Mexico, Philippines, Singapore and Taiwan, plus the USA. This DTIA assumes that Dutch public sector customers do not give such consent. Therefore transfer to the first list of subprocessors is out of scope. 2. However, even if a customer does not consent to transfer personal data to solve a support ticket, Google engineers may still have limited, authorized access to Diagnostic Data for infrastructure maintenance and troubleshooting all kinds of technical issues, and to remediate customer-initated support requests. Google uses subprocessors in 7 third countries that may have access to the Diagnostic Data: Australia, Brazil, Chile, Hong Kong, India, Singapore and Taiwan. Additionally, access may be obtained from the USA. See https://workspace.google.com/terms/subprocessors.html for Google's public documentation. Google has provided confidential information relating to its subprocessors and affiliates to SURF and SIVON. Google has explained the probability of this transfer is very low: "Google service maintenance engineers located in Australia, Brazil, Chile, Hong Kong, India, Singapore, or Taiwan have not accessed any Google Meet Customer Data or Service Data belonging to public sector or education institutions located in the Netherlands in the past two years."	Note Privacy Company: Google does not ask for specific consent for the transfer of Content Data to employees in the first list of 12 third countries: the support employees only asks for consent to access to Content or Service Data of the customer without informing the customer in what country they operate. **That is why this DTIA assumes that schools and universities will not provide such consent.**
f)	Categories of data subjects concerned:	Google Workspace administrators, students and employee users of Dutch education and research organisations + external participants in Meet conferences (as guest users, or with a Google account).	
g)	Categories of personal data transferred:	The Service Data should be limited to regular personal data, if Dutch public sector customers follow the recommendations to (1) not include personal data or confidential information in the name of the Meet and (2) use pseudonyms for specific employees and students whose identity should remain confidential. There are two exceptions, when the Service Data may include data of a sensitive nature: (1) the account names of guest users cannot be pseudonymised and (2) frequent Meets in a short period of time between different government security officers may reveal cyber incidents.	
h)	Sensitive and special categories of personal data:	See row 10.	
i)	Technical implementation of the transfer:	Google does not provide an option to any its Workspace customers (free or paid) to select datacentres in the EU to process the Service Data, as these data are not mentioned on Google's limitative list of services and Content Data for which a Data Region choice is available. See: Google, Data regions: Choose a geographic location for your data, URL: https://support.google.com/a/answer/7630496?hl=en. This means the Service Data may be transferred to the 7 third countries as well as the USA where Google processes Service Data.	
j)	Technical and organizational measures in place:	Technical measures: Google uses its own encryption in transit for inter-region data traffic and global routing (ALTS and TLS, plus the MTA-STS standard for mail), and AED for data stored at rest. Two technical measures available for Content Data are not available for Service Data: the additional protection of Access Approval to explicitly approve access to recordings and transcripts stored in Drive and Client Side Encryption (CSE) for Meet. It follows from the technical investigation that the account name of the organiser is not just part of the Content Data (called 'Customer Data' by Google), but also part of the Diagnostic Data, as the directly identifiable Account Name of the organiser leaked to Google as part of unencrypted Telemetry Data. Additionally, the Google accounts of guest users in meetings organised by a government organisation or educational institution are not covered by the additional data protection measures such as Sovereign Controls. This means Google can process the information that a guest user has participated in a Meet organised by a Dutch public sector organisation, for its own purposes, as covered in Google's general (consumer) Privacy Policy. Organisational measures: Same as Content and Account Data	
k)	Relevant onward transfer(s) of personal data (if any):	Diagnostic Data from Meet may be transferred to 7 third countries for data center operations, software and systems engineering, maintenance and troubleshooting.	
l)	Countries of recipients of relevant onward transfer(s):	Australia, Brazil, Chile, Hong Kong, India, Singapore and Taiwan. Additionally, access may be obtained from the USA (no longer a third country)	

Step 2: Define the DTIA parameters

			Rationale
a)	Starting date of the transfer:	[assessment made on 28 November 2023]	
b)	Assessment period in years:	2	
c)	Ending date of the assessment based on the above:	X+2	
d)	Target jurisdiction for which the DTIA is made:	Australia, Brasil, Chile, Hong Kong, India, Singapore and Taiwan + United States	This includes access to Service Data for service maintenance and for technical support by engineers in these 7 third countries. It is assumed that Dutch public sector Workspace customers will not consent to transfer of Service Data to the other list of subprocessors in 12 third countries in the context of a support request.
e)	Is importer an Electronic Communications Service Provider as defined in	Yes	
f)	Does importer/processor commit to legally resist every request for access:	No	Google explains in its "Government Requests for Cloud Customer Data" whitepaper that it commits to object to, or limit or modify, any legal process that it reasonably determines to be overbroad, disproportionate, incompatible with applicable law, or otherwise unlawful. See Step 2 on page 7. However, this guide does not cover the Service Data. The confidential agreements with the Dutch Education customers include detailed commitments with regard to disclosure. Google has also explained in reply to this DTIA that it incidentally responds - voluntarily - to a request from a Third Country authority by disclosing very limited EEA personal data in emergency situations where it has a good faith belief that disclosure of EEA personal data to a Third Country government authority is necessary to prevent an imminent threat to life or serious physical injury. The Dutch Education sector does not agree that Google is entitled to such voluntary disclosures. Google has assured the Dutch education sector that it has not disclosed any personal data from Dutch Education customers in the past 2 years for this purpose.
g)	Relevant local laws taken into consideration:	Google has not shared its legal analysis of applicable laws and their compliance with the fundamental right guarantees offered to data subjects in Australia, Brasil, Chile, Hong Kong, India, Singapore and Taiwan.	This DTIA cannot provide a detailed legal analysis of the applicable surveillance laws in the 7 third countries. Absent such an analysis, it has to be assumed that some or all authorities in the third countries are permitted to obtain data from Google. Since the adequacy decision for the USA from the European Commission on 10 July 2023, transfers to the USA based on the DPF do not have to be complemented by supplementary measures. The Assessment has already been made by the European Commission, meaning that when the DPF applies, an additional assessment is not necessary. However, as controller the Dutch government still needs to assess the risks in all third final destination countries.

Step 3: Probability that a foreign authority has a legal claim in the data and wishes to enforce it against the provider

		Probability	Cases	Cases remaining	Rationale
a)	Number of cases under the laws listed in Step 2g per year in which an authority in the third countries is estimated to attempt to obtain relevant data through legal action during the period under consideration.	100%	1,00		In reply to this DTIA Google has stated it has not disclosed any Diagnostic Data (as part of Service Data) from Dutch Education customers to law enforcement in the past two years: "We can confirm that, in the past two years (which we understand to be your 'assessment period'), we have not disclosed any Customer Data or Service Data belonging to public sector or education institutions located in the Netherlands in response to requests from law enforcement agencies (such as requests made under warrant or subpoena) based in Australia; Brazil; Chile; Hong Kong; India; Singapore; Taiwan; or the United States (US)." Google has also explicitly confirmed it has not voluntarily disclosed any personal data from Dutch Education customers in the past 2 years. Google does not provide information if Diagnostic Data from EU public sector customers were disclosed to security services and intelligence agencies. Google only mentions a range between 0 and 499 at https://transparencyreport.google.com/user-data/us-national-security. For clarity, under US law, providers can neither confirm nor deny having received any specific legal demands subject to a secrecy obligation. It is plausible that the other third countries have similar secrecy obligations. Google is contractually committed to redirect orders for disclosure to its customers. If not possible, Google will evaluate if it is valid and binding order, If compelled to disclose personal data, Google will try to notify the customer and allow the customer to challenge the request, where legally permitted. URL: https://services.google.com/fh/files/blogs/government_access_technical_whitepaper.pdf The probability of such compelled disclosure cannot be set to zero. Absent more transparency about disclosure to security services and intelligence agencies the probability is set to 1 case per year.
b)	Share of such cases in which the request occurs in connection with a case that due to its nature in principle permits the authority to obtain the data also from a provider	100%	1,00		Absent a detailed analysis of applicable laws in the 7 third countries, it has to be assumed that some or all authorities in the third countries are permitted to obtain data from Google. For example, as Hong Kong is part of China, governments across the EU have expressed concerns about access by Chinese authorities to personal data from EU citizens. As quoted above, though Google has not disclosed any Dutch Education Diagnostic Data to law enforcement authorities in these countries in the past 2 years, disclosure to intelligence/security services or voluntary disclosure cannot be excluded.
c)	Probability that in the remaining such cases it will be possible for the company to successfully cause the authority (by legal means or otherwise) to give up its request for the data **in plain text**	0%	1,00		CSE is not available for Diagnostic Data. Therefore, the probability that Google is not able to produce these data in clear text, is zero.
d)	Probability that in the remaining cases the requested data will be provided in one way or another (e.g., with consent or through legal or administrative assistance)	1%	0,99		Absent an MLAT with the third country, EU organisations cannot consent to disclose Diagnostic Data to a government authority in a third country, based on Art 48 GDPR. Google has explained in reply to this DTIA that it has not provided any personal data from Dutch Education customers to law enforcement authorities in the assessment period, also not on a voluntary basis.
e)	Probability that in the remaining cases the authority will consider the data it is seeking to be so important that it will look for another way to obtain it	50%	0,50	0,50	Enforcing lawful access via Google to access Diagnostic Data of one of its Education customers (where it is a processor) is much more difficult than in the case of data of private individuals (where it is a controller). It also takes time. Therefore, we believe that the authorities will want to undergo such trouble only in particularly important cases, thus significantly reducing the number of relevant cases. The probability is set to 50%, similar as the Content, Account and Website Data.
	Number of cases per year in which the question of lawful access by a foreign authority arises			0,50	Based on E35, which is a calculation of C35*D34. D34 is calculated as (1-C34)*D33
	Number of cases in the period under consideration			0,99	Based on E37*C21

Step 4a: Probability that a foreign authority will successfully enforce the claim through the provider

Legal Basis considered for the following assessment: Unknown for Australia, Brasil, Chile, Hong Kong, India, Singapore and Taiwan, EU Adequacy Decision for registered participants in the EU-US Data Privacy Framework

	Prerequisite for success	Probability per case			Rationale
a)	Probability that the authority is aware of the provider and its	100%		100%	Google is a well-known cloud services provider with a substantial amount of Workspace for Education Plus Customers in the EU
b)	Probability that an employee of the provider or its subcontractors will gain access to the data in plain text in a support-case ... (prerequisite no. 2)	0%	0,00%		Customers can intentionally, with consent, allow Google support employees in 12 third countries to access Diagnostic Data in plain text as part of a support request. It is assumed that Dutch public sector Workspace customers will not consent to such a transfer. However, the Support Data can also be accessed without such consent by subprocessors in Australia, Brasil, Chile, Hong Kong, India, Singapore and Taiwan, as part of technical service maintenance and support, but they need to be authorised to access specific data [see below]. Schools and universities can cannot prevent access to Support Data by the support engineers in these 7 third countries if they file a support request. They can only lower the probability of access for this purpose by never filing a support request with Google. However, that doesn't end the transfer. Google engineers in the 7 third countries may still have access to some personal data relevant for troubleshooting, releasing new code, making configuration changes or emergency maintenance purposes. Google has explained that customers can view the availability stats of Meet in the Netherlands to make an estimate of the probability of such transfers. These stats show an average uptime of 99.993 per cent. That means Meet is down for an average of 3 minutes per month, or, only available for 1 hour and 15 minutes in total during the last 2 years.
	... and is able to search for, find and copy the data requested by the authority (prerequisite no. 3)	1%		5%	Google employees can incidentally be tasked to look at problems from Dutch customers with Meet, but they cannot 'search' for any customers' personal data, including Diagnostic Data. Google explains: "Access is entirely dependent on the specific activity they need to perform and only occurs where absolutely necessary to e.g. address the specific technical issue they are investigating." Google has taken many access control measures. Google explains: "An employee's authorization settings are used to control access to all resources, including Customer Data, Service Data and Google Meet systems. Even if an employee has the appropriate authorization to access Customer Data or Service Data, they must still provide a justification tied to a specific technical issue otherwise access to that data will be rejected. All technical issues are individually tracked using a unique case ID, and employee justifications are periodically reviewed. **This means that it is not technically possible for an employee to access Customer Data or Service Data that is not required for them to investigate and resolve specific technical issues tasked to them.** Access is monitored by our dedicated security teams as a check on the effectiveness of our controls. The security teams actively monitor access patterns and investigate unusual events." In reply to a question from Privacy Company about log controls, Google stated it has "**not detected any unauthorised usage by engineers in the third countries in the past 2 years to a) Customer Data and b) Service Data."**
c)	Probability that despite the technical countermeasures taken, employees of the provider, of its subcontractors or of the parent company technically have access to data in plain text (also) outside a support situation (e.g., using admin privileges) or are able to gain such access, e.g., by covertly installing a backdoor or "hacking" into the system (irrespective of whether they are allowed to do so) ... (prerequisite no. 2)	10%	5,00%		As analysed above, CSE cannot be applied to Diagnostic Data. Though Google has not provided any personal data from Dutch Education customers to law enforcement in the past 2 years, Google is prohibited from publishing details about disclosure to security services. In reply to this DTIA Google has explained it has not built in any backdoors. "Google has not provided any government with direct access to any information stored in our data centers, including data stored or processed by the Meet application." Google has also stated: "Google has not joined any program that would give the U.S. government—or any other government—direct access to its servers." Google has clarified that this statement also applies to indirect access through for example, distribution of a new version or temporary lifting of transit encryption. "Google will not disable security features or alter Meet systems to allow third parties to gain access to Customer Personal Data that would otherwise be unavailable to a third party in clear text." In view of the strict access controls described in row 47 and the fact that Google has not detected any unauthorised usage by engineers in the past 2 years, the probability of access to the Diagnostic Data n plain text is estimated to be a maximum of 10%, based on the assumption that authorities in the third countries do have legal powers to compel Google to decrypt with its own keys, and to disclose these data.
	... and are then able to search for, find and copy the data requested by the	50%			It is not certain that Google would succeed in gaining access and be able to search for the Diagnostic Data specifically requested by an authority.
d)	Probability that the provider, the subcontractor or its parent company, respectively, is located within the jurisdiction of the authority (prerequisite no. 4)	100%		100%	Google explains in its information about subprocessors that its subsidiaries in 7 third countries may have access to the Diagnostic Data for the purposes of data centre operations, and for software and systems engineering, maintenance and troubleshooting. See: https://workspace.google.com/terms/subprocessors.html

e)	Probability that despite the technically limited access and the technical and organizational countermeasures in place, the authority is permitted to order the provider, its subcontractor or the parent company, respectively, to obtain access to the data and produce it to the authority in plain text (prerequisite no. 5)	100%	100%	*Speculative estimate. Though Google by default applies encryption to data-at-rest, including Diagnostic Data, Google has access to these keys, can use these keys to decrypt if necessary for troubleshooting, and can hence also be ordered to decrypt the data. Therefore the probability that government authorities in the third countries can order Google to provide access to the Diagnostic Data is set to 100%.*
f)	Probability that if data were to be handed over to the foreign authority, this would lead to the criminal liability of employees of the provider or its subcontractors, the prosecution of which would be possible and realistic, and as a consequence, the data does not have to be produced or is not produced (prerequisite no. 6)	25%	75%	*Privacy Company has studied the confidential SOC-2 and C5:2020 audit reports, but these reports only assess Google's compliance with these standards for Content Data, not for the Diagnostic Data Google includes in the term Service Data. The probabiilty is not zero, because Google has a Code of Conduct, which mentions the existence of anti-bribery laws, with the following sentence: "Like all businesses, Google is subject to lots of laws, both U.S. and non-U.S., that prohibit bribery in virtually every kind of commercial setting." URL: https://abc.xyz/investor/google-code-of-conduct/* *All Google employees are required to follow this Code. The probability is set to 50% because the (existence of) anti bribery laws in the 7 third countries is unknown.*
g)	Probability that the government organisation does not succeed in removing the relevant data in time or otherwise withdrawing it from the provider's access (prerequisite no. 7)	100%	100%	*Google has explained in the past 2 years it has **not disclosed any Diagnostic Data** belonging to public sector or education institutions located in the Netherlands in response to requests from law enforcement agencies (such as requests made under warrant or subpoena) based in Australia; Brazil; Chile; Hong Kong; India; Singapore; Taiwan; or the United States (US). However, Google does not disclose statistics about disclosure to security services/intelligence agencies. It is plausible that Google will be subjected to gagging orders from security services, and not permitted to inform its Customer. Hence Google may not be in a position to issue a timely warning to its customer. The probability is set to 100% absent an explanation from Google.*

Residual risk of successful lawful access by a foreign authority through the provider (given the countermeasures): 3,75% Result of multiplication of E45*E46*E50*E51*E52*E53

Step 4b: Probability of foreign lawful access by mass surveillance of contents

Legal Basis considered for the following assessment: Unknown for Australia, Brasil, Chile, Hong Kong, India, Singapore and Taiwan, EU Adequacy Decision for registered participants in the EU-US Data Privacy Framework including FISA

		Probability in the period			**Rationale**
a)	Probability that the data at issue is transmitted to the provider or its subcontractors in a manner that permits the telecommunications providers in the country to view it in plain text as part of an upstream monitoring of Internet backbones	0%	0,00%	0,10%	*Google applies encryption in transit for inter-region data traffic and global routing (ALTS and TLS, plus the MTA-STS standard for mail), and AED for data stored at rest. Google also writes it never gives any government "backdoor" access." In reply to questions about access to encryption keys as part of 'backdoors', Google has further clarified: "Google will not disable security features or alter Meet systems to allow third parties to gain access to Customer Personal Data that would otherwise be unavailable to a third party in clear text."*
b)	Probability that the data transmitted will include content picked by	0%			*See the explanation in the row above.*
c)	Probability that the provider or a subcontractor in the country is	10%	0,10%		*As Google applies the encryption, Google and its subsidiaries are technically capable of lifting that encryption, and can do so in practice for service*
d)	Probability that the provider or a subcontractor in the countries above may be legally required to perform such as search (also) with the company's data	1%			*Speculative estimate. This refers to Upstream Data Collection. According to the Adequacy Decision from the European Commission, personal data may be transferred to companies in the USA certified under the DPF without having to put additional supplementary measures (as described by the European Court of Justice and in the recommendations from the EDPB) in place.* *It is plausible that some Diagnostic Data from a Dutch government organisation or school/university are interesting for security services in the 7 third countries where they may be accessed. This probability is low based on Google's statement that it has **not provided any government with direct access to any information stored in its data centers, including data stored or processed by the Meet application (i.e. including direct access for security services).***
e)	Probability that the data is regarded as content that is the subject of intelligence searches in the country as per the above laws	100%			*It is plausible that Diagnostic Data from a Dutch education organisation are interesting for security services in the 7 third countries where they may be accessed. Since customers cannot encrypt Diagnostic Data with their own key, and Diagnostic Data reveal who communicates with whom and when, these data are more likely to be regarded as interesting information than the Content, Support or Website Data.*

Residual risk of successful lawful access by a foreign intelligence service without any guarantee of legal recourse (in view of the countermeasures): 0,10%

Step 5: Overall assessment

Probability that the question of lawful access via the cloud provider will arise at all (1 case in the period = 100%)	99,00%
Probability of successful lawful access by the foreign authorities concerned in these cases despite the countermeasures	3,75%
Probability of additional successful lawful access by a foreign intelligence service where there is no guarantee of legal recourse (despite countermeasures)	0,10%
Overall probability of a successful lawful access to data in plain text via the cloud provider in the observation period:	3,81%
Description in words (based on Hillson*):	Very low
The number of years it takes for a lawful access to occur at least once with a **90 percent** probability:	118
The number of years it takes for a lawful access to occur at least once with a **50 percent** probability:	36

... assuming that the probability neither increases nor decreases over time (like tossing a coin)

** Scale: <5% = "Very low", 5-10% = "Low", 11-25 = "Medium", 26-50% = "High" and >50% = "Very high" (by David Hillson, 2005, see https://www.pmi.org/learning/library/describing-probability-limitations-natural-language-7556).*

Step 6: Data subject risks

				Rationale
a)	*Estimated probability of occurrence of successful lawful access risk:*	*3,81%* *3= regular personal data in the clear*	*Very Low* *High*	*This assessment assumes Dutch public sector organisations will follow the recommendation to use pseudonyms for specific employees and students that incur a high data protection risk if there is unauthorised access to their data. Hence, the Diagnostic Data should only contain pseudonymised and regular personal data (in the service generated server logs). Though the impact of unauthorised access to regular personal data is still high, the risk is assessed as low in view of the very low probability that the risk materialises.*
b)	*Estimated impact of risk*			

Very High	Low	High	High	High	High
High	Low	Medium	High	High	High
Medium	Low	Medium	Medium	High	High
Low	Low	Low	Medium	Medium	High
Very Low	Low	Low	Low	Low	High
	0	1	2	3	4

Low

Step 7: Define the safeguards in place

				Rationale
a)	Would it be feasible, from a practical, technical and economical point of view, for the data exporter to transfer the personal data in question to a location in a whitelisted country instead?	Yes	*Describe why you still do not pursue this option*	*Google does not make a Data Region choice available for Diagnostic Data as part of the Service Data. Google has not disclosed any plans to limit this access to EU-based engineers only. This means the Diagnostic Data can be processed by support engineers in the USA, and in the 7 third countries.*
b)	Is the personal data transferred under one of the exemptions pursuant to applicable data protection law (e.g., Art. 49 GDPR in case of the GDPR)?	No		*Once an education organisation uses Google Meet, the transfer of Diagnostic Data is structural, not incidental.*
c)	Is the personal data at issue transmitted to the target jurisdiction in clear text (i.e. there is no appropriate encryption in-transit)?	No	*Ensure that data remains encrypted*	*No, Google by default applies encryption both in-transit and to stored data, but with its own keys. It is not possible to apply CSE to the Diagnostic Data.*
d)	Is the personal data at issue accessible in the target jurisdiction in clear text by the data importer/recipient or a third party (i.e. the data is either not appropriately encrypted or access to the keys to decrypt is possible)?	Yes	*Foreign lawful access is at least technically possible*	*Yes, Google and its subsidiaries in 3d countries can technically access the unencrypted Diagnostic Data, although this would be a violation of policy and organisational measures.*
e)	Is the personal data at issue protected by a transfer mechanism approved by the applicable data protection law (e.g., the EU Standard Contractual Clauses in case of the GDPR, approved BCR, or - in the case of an onward transfer - a back-to-back-contract in line with the EU SCCs), and can you expect compliance with it, insofar permitted by the target jurisdiction, and judicial enforcement (where applicable)?	Yes	*Ensure that the mechanism remains in place and is complied with*	*The Dutch education customers rely on appropriate transfer mechanisms under Chapter V GDPR.*

Based on the answers given above, the transfer is: permitted

Final Step: Conclusion

In view of the above and the applicable data protection laws, the transfer is: permitted

Reassess at the latest by: X+2
(or if there are any changes in circumstances)

This Transfer Impact Assessment has been made by:
SLM Rijk / SURF / SIVON / PRIVACY COMPANY

Place, Date:
Signed:
By: [School or University X]

Data Transfer Impact Assessment (DTIA) on the transfer to third countries of Security Data and notifications processed by Google Meet (audio/video conferencing)

This tab describes the transfers of Security logfiles, and reports processed by Google's Trust & Safety team to the USA. Google considers these security data a subsection of Service Data. This DTIA distinguishes between 5 categories of Service Data: data about support tickets, Account Data, Diagnostic Data, Security Data and Website Data. Because there are differences in both the impact and the probability of unauthorised access to these data, this DTIA continues to distinguish between 6 categories of personal data. This distinction also make this DTIA more comparable with other public DTIAs on videoconferencing services.

Step 1: Describe the intended transfer			**COMMENTS GOOGLE**
a)	Data exporter (or the sender in case of a relevant onward transfer):	Dutch education and research organisation [X]	
b)	Country of data exporter:	**[Confidential]** for the Dutch education sector.	
c)	Data importer (or the recipient in case of a relevant onward transfer):	Google LLC in the USA. The Dutch education customers rely on appropriate transfer mechanisms under Chapter V GDPR.	
d)	Country of data importer:	USA The contracting entity for Dutch education customers of Google Workspace is **Google Cloud EMEA Limited** (see https://cloud.google.com/terms/google-entity), a Google entity based in Dublin, Ireland. Google Cloud EMEA Limited is a wholly owned subsidiary of Google LLC, which in turn is a wholly owned subsidiary of Alphabet Inc.	
e)	Context and purpose of the transfer:	This assessment is based on the exclusive transfer of Security logs and notifications to the Trust & Safety Team in the USA. Based on the adequacy decision for the data protection regime in the USA, organisations do not have to take extra measures to protect the personal data.	
f)	Categories of data subjects concerned:	Google Workspace administrators, students and employee users of Dutch education and research organisations + external participants in Meet conferences (as guest users, or with a Google account).	
g)	Categories of personal data transferred:	Security logs may reveal information about malicious attackers, such as their IP addresses and types of devices used. Reports to the Trust & Safety Team, as well as flags of suspected CSAM may include regular, sensitive and special categories of data.	
h)	Sensitive and special categories of personal data:	Security logs may be used for criminal investigation, reports and flags may include sensitive and special categories of data, as well as data about (alleged) criminal offenses.	
i)	Technical implementation of the transfer:	Security logs are kept by Google LLC in the USA. The Trust & Safety team works in the USA. Google has confirmed it does not use AI to scan for unknown CSAM material, and has committed to comply with the guidance from the EDPB and future new CSAM legislation in the EU.	
j)	Technical and organizational measures in place:	No additional technical and organisational measures are required for the transfer to the USA since the adequacy decision from the European Commission on 10 July 2023. The Dutch education sector has negotiated guarantees from Google with regard to the procedure to be followed if Google were to receive an order from a government authority for these data. The framework contract includes sufficient contractual solutions addressing this topic.	
k)	Relevant onward transfer(s) of personal data (if any):	USA	
l)	Countries of recipients of relevant onward transfer(s):	USA	

Step 2: Define the DTIA parameters			**Rationale**
a)	Starting date of the transfer:	[assessment made on 28 November 2023]	
b)	Assessment period in years:	2	
c)	Ending date of the assessment based on the above:	X+2	
d)	Target jurisdiction for which the DTIA is made:	United States (exclusively)	
e)	Is importer an Electronic Communications Service Provider as defined in	Yes	
f)	Does importer/processor commit to legally resist every request for access:	No	*Google explains in its "Government Requests for Cloud Customer Data" whitepaper that it commits to object to, or limit or modify, any legal process that it reasonably determines to be overbroad, disproportionate, incompatible with applicable law, or otherwise unlawful. See Step 2 on page 7. However, this guide does not cover the Service Data.* *The confidential agreements with the Dutch Education customers include detailed commitments with regard to disclosure. Google has also explained in reply to this DTIA that it incidentally responds - voluntarily - to a request from a Third Country authority by disclosing very limited EEA personal data in emergency situations where it has a good faith belief that disclosure of EEA personal data to a Third Country government authority is necessary to prevent an imminent threat to life or serious physical injury. The Dutch Education sector does not agree that Google is entitled to such voluntary disclosures. Google has assured the Dutch education sector that it has not disclosed any personal data from Dutch Education customers in the past 2 years for this purpose.*
g)	Relevant local laws taken into consideration:	For the transfer to the USA, the updated relevant US laws are analysed by the European Commission in the Data Privacy Framework decision from 10 July 2023.	*Since the adequacy decision for the USA from the European Commission on 10 July 2023, transfers to the USA based on the DPF do not have to be complemented by supplementary measures. The assessment has already been made by the European Commission.*

Step 7: Define the safeguards in place				**Rationale**
a)	Would it be feasible, from a practical, technical and economical point of view, for the data exporter to transfer the personal data in question to a location in a whitelisted country instead?	Yes	*Describe why you still do not pursue this option*	*Like other hyperscalers, Google operates centralised security services and one Trust and Safety Team in the USA. Though technically possible, Google has no intention to create specific EU security and trust & safety teams.*
b)	Is the personal data transferred under one of the exemptions pursuant to applicable data protection law (e.g., Art. 49 GDPR in case of the GDPR)?	No		*Once an education organisation uses Google Meet the transfer is structural, not incidental.*
c)	Is the personal data at issue transmitted to the target jurisdiction in clear text (i.e. there is no appropriate encryption in-transit)?	No	*Ensure that data remains encrypted*	*No, Google by default applies encryption both in-transit and to stored data, but with its own keys.*
d)	Is the personal data at issue accessible in the target jurisdiction in clear text by the data importer/recipient or a third party (i.e. the data is either not appropriately encrypted or access to the keys to decrypt is possible)?	Yes	*Foreign lawful access is at least technically possible*	*Yes, authorised Google employees in the USA can technically access the security logs and data for the trust & safety team.*
e)	Is the personal data at issue protected by a transfer mechanism approved by the applicable data protection law (e.g., the EU Standard Contractual Clauses in case of the GDPR, approved BCR, or - in the case of an onward transfer - a back-to-back-contract in line with the EU SCCs), and can you expect compliance with it, insofar permitted by the target jurisdiction, and judicial enforcement (where applicable)?	Yes	*Ensure that the mechanism remains in place and is complied with*	*The Dutch education customers rely on appropriate transfer mechanisms under Chapter V GDPR.*

Based on the answers given above, the transfer is: Permitted

Final Step: Conclusion

In view of the above and the applicable data protection laws, the transfer is: **permitted**

Reassess at the latest by: X+2

(or if there are any changes in circumstances)

This Transfer Impact Assessment has been made by:
SLM Rijk / SURF / SIVON / PRIVACY COMPANY

Place, Date:
Signed: ____________________
By: [School or University X]

Data Transfer Impact Assessment (DTIA) on the transfer to third countries of Website Data processed by Google Meet (audio/video conferencing)

This DTIA was made by Privacy Company, SLM Rijk, SURF and SIVON, using and adapting the template provided by David Rosenthal, provided under CC license

This tab describes the transfers of Website Data, both when end-users (logged-in users and guest users) participate via their browser in Google Meet, and when admins to access the Admin Console. Google considers Website Data a subsection of Service Data. This DTIA distinguishes between 5 categories of Service Data: data about support tickets, Account Data, Diagnostic Data, Security Data and Website Data. Because there are differences in both the impact and the probability of unauthorised access to these personal data, this DTIA continues to distinguish between 6 categories of personal data. This distinction also make this DTIA more comparable with other public DTIAs on videoconferencing services.

Step 1: Describe the intended transfer

			COMMENTS GOOGLE
a)	Data exporter (or the sender in case of a relevant onward transfer):	Dutch education and research organisation [X]	
b)	Country of data exporter:	**[Confidential]** for the Dutch education sector.	Technically, Google maintains servers around the world and its support and service engineers in the 7 third countries can access data anywhere, if necessary and authorised.
c)	Data importer (or the recipient in case of a relevant onward transfer):	Google LLC in the USA. The Dutch education customers rely on appropriate transfer mechanisms under Chapter V GDPR.	
d)	Country of data importer:	USA, with onward transfers to third countries for recorded data. The contracting entity for Dutch education customers of Google Workspace is **Google Cloud EMEA Limited** (see https://cloud.google.com/terms/google-entity), a Google entity based in Dublin, Ireland. Google Cloud EMEA Limited is a wholly owned subsidiary of Google LLC, which in turn is a wholly owned subsidiary of Alphabet Inc.	
e)	Context and purpose of the transfer:	Google Meet (https://apps.google.com/intl/en/meet/) provides the ability to organise and participate in video conferences, which can consist of 1-on-1 or group calls (up to 500 participants) with both audio and video or just audio. The video conference service also offers related features such as text chatting and file sharing among participants, (AI generated) live captions of speech, and (AI) translations of live captions. This tab is about the specific webserver access logs maintained by Google with personal data about the access by unauthenticated end-users to the login-page, by authenticated visitors of the entry page in a browser to participate in Meet and by admins to the Admin Console. Google also uses a NID-cookie with a unique identifier when users sign-in to their Google Workspace for Education account, or when a user wants to read the legal information in Google's Cloud Privacy Notice. Google has explained it will not use the NID-cookie set in Workspace for Education for advertising purposes, nor inside Workspace, nor on external (third party) websites if the user has not provided consent for non-essential cookies, and will improve its cookie banner on the legal page by [Confidential]. Website Data may be stored in or accessed from multiple third countries and the United States. In its Data Transfer policy Google writes: "We maintain servers around the world and your information may be processed on servers located outside of the country where you live." URL: https://policies.google.com/privacy/frameworks. Google allows its Workspace Education customers to select datacentres in the EU to process the Content Data from Meet, but such a data region choice is not available for the Website Data (which for Google are part of 'Service Data'). Google has clarified that sub-processors and subsidiaries that are given access to Content Data (Customer Data) also have access to Service Data. Therefore, the Website Data can be transferred in two circumstances: 1. If a customer explicitly elects to enable such access to for example audit logs or a crash log to help a Google support engineer solve the issue. In that case, the Website Data may be transferred to 12 third countries (without an adequacy decision from the EU): Australia, Brazil, Chile, El Salvador, Guatemala, Hong Kong, India, Malaysia, Mexico, Philippines, Singapore and Taiwan, plus the USA. This DTIA assumes that Dutch public sector customers do not give such consent. Therefore transfer to the first list of subprocessors is out of scope. 2. However, even if a customer does not consent to transfer personal data to solve a support ticket, Google engineers may still have limited, authorized access to Website Data for infrastructure maintenance and troubleshooting all kinds of technical issues, and to remediate customer-initiated support requests. Google uses subprocessors in 7 third countries that may have access to the Website Data: Australia, Brazil, Chile, Hong Kong, India, Singapore and Taiwan. Additionally, access may be obtained from the USA. See https://workspace.google.com/terms/subprocessors.html for Google's public documentation. Google has provided confidential information relating to its subprocessors and affiliates to SURF and SIVON. Google has explained the probability of this transfer is very low: "Google service maintenance engineers located in Australia, Brazil, Chile, Hong Kong, India, Singapore, or Taiwan have not accessed any Google Meet Customer	Google has not answered the question if Website Data (including IP addresses) from guest users in meetings organised by Education customers are offered the same processing guarantees. This DTIA assumes there is no such protection umbrella.
f)	Categories of data subjects concerned:	Google Workspace administrators, students and employee users of Dutch education and research organisations + external participants in Meet conferences (as guest users, or with a Google account).	
g)	Categories of personal data transferred:	The Website Data (as defined in bold in row 8 e) should be limited to pseudonymised personal data, if Dutch public sector customers follow the recommendation to use pseudonyms for admins, employees and students whose identity should remain confidential.	
h)	Sensitive and special categories of personal data:	none	
i)	Technical implementation of the transfer:	Google does not provide an option to any its Workspace customers (free or paid) to select datacentres in the EU to process the Website Data, as the accounts are not mentioned on Google's limitative list of services for which a Data Region choice is available. See: Google, Data regions: Choose a geographic location for your data, URL: https://support.google.com/a/answer/7630496?hl=en. This means the Website Data may be transferred to the 7 third countries as well as the USA where Google processes Service Data.	
j)	Technical and organizational measures in place:	**Technical measures:** Google uses its own encryption in transit for inter-region data traffic and global routing (ALTS and TLS, plus the MTA-STS standard for mail), and AED for data stored at rest. The technical measure of Access Approval is only available for Content Data, not for the Website Data. **Organisational measures**: Same as Content and Account Data	
k)	Relevant onward transfer(s) of personal data (if any):	Website Data from Meet may be transferred to 7 third countries for data center operations, software and systems engineering, maintenance and troubleshooting.	
l)	Countries of recipients of relevant onward transfer(s):	Australia, Brazil, Chile, Hong Kong, India, Singapore and Taiwan. Additionally, access may be obtained from the USA (no longer a third country)	

Step 2: Define the DTIA parameters

			Rationale
a)	Starting date of the transfer:	[assessment made on 28 November 2023]	
b)	Assessment period in years:	2	
c)	Ending date of the assessment based on the above:	X+2	
d)	Target jurisdiction for which the DTIA is made:	Australia, Brazil, Chile, Hong Kong, India, Singapore and Taiwan + United States	*This includes access to Website Data for service maintenance and for technical support by engineers in these 7 third countries. It is assumed that Dutch public sector Workspace customers will not consent to transfer of Service Data to the other list of subprocessors in 12 third countries in the context of a support request.*
e)	Is importer an Electronic Communications Service Provider as defined in	Yes	
f)	Does importer/processor commit to legally resist every request for access:	No	*Google explains in its "Government Requests for Cloud Customer Data" whitepaper that it commits to object to, or limit or modify, any legal process that it reasonably determines to be overbroad, disproportionate, incompatible with applicable law, or otherwise unlawful. See Step 2 on page 7. However, this guide does not cover the Website Data.* *The confidential agreements with the Dutch Education customers include detailed commitments with regard to disclosure. Google has also explained in reply to this DTIA that it incidentally responds - voluntarily - to a request from a Third Country authority by disclosing very limited EEA personal data in emergency situations where it has a good faith belief that disclosure of EEA personal data to a Third Country government authority is necessary to prevent an imminent threat to life or serious physical injury. The Dutch Education sector does not agree that Google is entitled to such voluntary disclosures. Google has assured the Dutch education sector that it has not disclosed any personal data from Dutch Education customers in the past 2 years for this purpose.*
g)	Relevant local laws taken into consideration:	Google has not shared its legal analysis of applicable laws and their compliance with the fundamental right guarantees offered to data subjects in Australia, Brasil, Chile, Hong Kong, India, Singapore and Taiwan.	*This DTIA cannot provide a detailed legal analysis of the applicable surveillance laws in the 7 third countries. Absent such an analysis, it has to be assumed that some or all authorities in the third countries are permitted to obtain data from Google.* *Since the adequacy decision for the USA from the European Commission on 10 July 2023, transfers to the USA based on the DPF do not have to be complemented by supplementary measures. The Assessment has already been made by the European Commission, meaning that when the DPF applies, an additional assessment is not necessary. However, as controller the Dutch government still needs to assess the risks in all third final destination countries.*

Step 3: Probability that a foreign authority has a legal claim in the data and wishes to enforce it against the provider

		Probability	Cases	Cases remaining	Rationale
a)	Number of cases under the laws listed in Step 2g per year in which an authority in the third countries is estimated to attempt to obtain relevant data through legal action during the period under consideration.	100%	1,00		*In reply to this DTIA Google has stated it has not disclosed any Website Data (as part of Service Data) from Dutch Education customers to law enforcement in the past two years: "We can confirm that, in the past two years (which we understand to be your 'assessment period'), we have not disclosed any Customer Data or Service Data belonging to public sector or education institutions located in the Netherlands in response to requests from law enforcement agencies (such as requests made under warrant or subpoena) based in Australia; Brazil; Chile; Hong Kong; India; Singapore; Taiwan; or the United States (US)."* *Google does not provide information if Website Data from EU customers were disclosed to security services and intelligence agencies. Google only mentions a range between 0 and 499 at https://transparencyreport.google.com/user-data/us-national-security. For clarity, under US law, providers can neither confirm nor deny having received any specific legal demands subject to a secrecy obligation. It is plausible that the other third countries have similar secrecy obligations.* *Google is contractually committed to redirect orders for disclosure to its customers. If not possible, Google will evaluate if it is valid and binding order, If compelled to disclose personal data, Google will try to notify the customer and allow the customer to challenge the request, where legally permitted. URL: https://services.google.com/fh/files/blogs/government_access_technical_whitepaper.pdf* *The probability of such compelled disclosure cannot be set to zero. Absent more transparency about disclosure to security services and intelligence agencies the probability is set to 1 case per year.*
b)	Share of such cases in which the request occurs in connection with a case that due to its nature in principle permits the authority to obtain the data also from a provider	100%	1,00		*Absent a detailed analysis of applicable laws in the 7 third countries, it has to be assumed that some or all authorities in the third countries are permitted to obtain data from Google. For example, as Hong Kong is part of China, governments across the EU have expressed concerns about access by Chinese authorities to personal data from EU citizens. As quoted above, though Google has not disclosed any Dutch Education restricted access Website Data to law enforcement authorities in these countries in the past 2 years, disclosure to intelligence/security services or voluntary disclosure cannot be excluded.*
c)	Probability that in the remaining such cases it will be possible for the company to successfully cause the authority (by legal means or otherwise) to give up its request for the data **in plain text**	0%	1,00		*CSE is not available for Website Data. Therefore, the probability that Google is not able to produce these data in clear text, is zero.*
d)	Probability that in the remaining cases the requested data will be provided in one way or another (e.g., with consent or through legal or administrative assistance)	10%	0,90		*Absent an MLAT with the third country, EU organisations cannot consent to disclose Website Data to a government authority in a third country, based on Art 48 GDPR. Google has explained in reply to this DTIA that it has not provided any personal data from Dutch Education customers to law enforcement authorities in the assessment period, also not on a voluntary basis.*
e)	Probability that in the remaining cases the authority will consider the data it is seeking to be so important that it will look for another way to obtain it	50%	0,45	0,45	*Enforcing lawful access via Google to access Website Data from end users and admins of one of its Education customers (where it is a processor) is much more difficult than in the case of data of guest users and Workspace users that have logged out, where Google is a controller). It also takes time. Therefore, we believe that the authorities will want to undergo such trouble only in particularly important cases, thus significantly reducing the number of relevant cases. The probability is set to 50%, similar as the Content, Account and Diagnostic Data.*
	Number of cases per year in which the question of lawful access by a foreign authority arises			0,45	Based on E35, which is a calculation of C35*D34. D34 is calculated as (1-C34)*D33
	Number of cases in the period under consideration			0,90	Based on E37*C21

Step 4a: Probability that a foreign authority will successfully enforce the claim through the provider

Legal Basis considered for the following assessment: Unknown for Australia, Brazil, Chile, Hong Kong, India, Singapore and Taiwan, EU Adequacy Decision for registered participants in the EU-US Data Privacy Framework including FISA

	Prerequisite for success	Probability per case			Rationale
a)	Probability that the authority is aware of the provider and its	100%		100%	*Google is a well-known cloud services provider with a substantial amount of Workspace for Education Plus Customers in the EU*
b)	Probability that an employee of the provider or its subcontractors will gain access to the data in plain text in a support-case ... (prerequisite no. 2)	0%	0,00%		*The Website Data can be accessed without consent from customers by subprocessors in Australia, Brazil, Chile, Hong Kong, India, Singapore and Taiwan for data centre operation and technical support purposes. Google has explained that customers can **view the availability stats of Meet in the Netherlands to make an estimate of the probability of such transfers. These stats show an average uptime of 99.993 per cent.** That means Meet is down for an average of 3 minutes per month, or, only available for 1 hour and 15 minutes in total during the last 2 years.*
	... and is able to search for, find and copy the data requested by the authority (prerequisite no. 3)	1%		5%	*Google employees can incidentally be tasked to look at problems from Dutch customers with Meet, but they cannot 'search' for any customers' personal data, including Diagnostic Data. Google explains: "Access is entirely dependent on the specific activity they need to perform and only occurs where absolutely necessary to e.g. address the specific technical issue they are investigating." Google has taken many access control measures. Google explains: "An employee's authorization settings are used to control access to all resources, including Customer Data, Service Data and Google Meet systems. Even if an employee has the appropriate authorization to access Customer Data or Service Data, they must still provide a justification tied to a specific technical issue otherwise access to that data will be rejected. All technical issues are individually tracked using a unique case ID, and employee justifications are periodically reviewed. **This means that it is not technically possible for an employee to access Customer Data or Service Data that is not required for them to investigate and resolve specific technical issues tasked to them**. Access is monitored by our dedicated security teams as a check on the effectiveness of our controls. The security teams actively monitor access patterns and investigate unusual events." In reply to a question from Privacy Company about log controls, Google stated it has "**not detected any unauthorised usage by engineers in the third countries in the past 2 years to a) Customer Data and b) Service Data."***
c)	Probability that despite the technical countermeasures taken, employees of the provider, of its subcontractors or of the parent company technically have access to data in plain text (also) outside a support situation (e.g., using admin privileges) or are able to gain such access, e.g., by covertly installing a backdoor or "hacking" into the system (irrespective of whether they are allowed to do so) ... (prerequisite no. 2)	10%	5,00%		*As analysed above, CSE cannot be applied to Website Data. Though Google has not provided any personal data from Dutch Education customers to law enforcement in the past 2 years, Google is prohibited from publishing details about disclosure to security services.* *In reply to this DTIA Google has explained it has not built in any backdoors. "Google has not provided any government with direct access to any information stored in our data centers, including data stored or processed by the Meet application." Google has also stated: "Google has not joined any program that would give the U.S. government—or any other government—direct access to its servers." Google has clarified that this statement also applies to indirect access through for example, distribution of a new version or temporary lifting of transit encryption. "Google will not disable security features or alter Meet systems to allow third parties to gain access to Customer Personal Data that would otherwise be unavailable to a third party in clear text." In view of the strict access controls described in row 47 and the fact that Google has not detected any unauthorised usage by engineers in the past 2 years, the probability of access to the Website Data n plain text is estimated to be a maximum of 10%, based on the assumption that authorities in the third countries do have legal powers to compel Google to decrypt with its own keys, and to disclose these data.*
	... and are then able to search for, find and copy the data requested by the	50%			*It is not certain that Google would succeed in gaining access and be able to search for the Website Data specifically requested by an*
d)	Probability that the provider, the subcontractor or its parent company, respectively, is located within the jurisdiction of the authority (prerequisite no. 4)	100%		100%	*Google explains in its information about subprocessors that its subsidiaries in 7 third countries may have access to the Diagnostic Data for data centre operations and for software and systems engineering, maintenance and troubleshooting. See: https://workspace.google.com/terms/subprocessors.html*
e)	Probability that despite the technically limited access and the technical and organizational countermeasures in place, the authority is permitted to order the provider, its subcontractor or the parent company, respectively, to obtain access to the data and produce it to the authority in plain text (prerequisite no. 5)	100%		100%	*Speculative estimate. Though Google by default applies encryption to data-at-rest, including Website Data, Google has access to these keys, can use these keys to decrypt if necessary for troubleshooting, and can hence also be ordered to decrypt the data. Therefore the probability that government authorities in the third countries can order Google to provide access to the Website Data is set to 100%.*
f)	Probability that if data were to be handed over to the foreign authority, this would lead to the criminal liability of employees of the provider or its subcontractors, the prosecution of which would be possible and realistic, and as a consequence, the data does not have to be produced or is not produced (prerequisite no. 6)	25%		75%	*Privacy Company has studied the confidential SOC-2 and C5:2020 audit reports, but these reports only assess Google's compliance with these standards for Content Data, not for the Website Data (as part of the Service Data). The probability is not zero, because Google has a Code of Conduct, which mentions the existence of anti-bribery laws, with the following sentence: "Like all businesses, Google is subject to lots of laws, both U.S. and non-U.S., that prohibit bribery in virtually every kind of commercial setting." URL: https://abc.xyz/investor/google-code-of-conduct/* *All Google employees are required to follow this Code. The probability is set to 50% because the (existence of) anti bribery laws in the 7 third countries is unknown.*
g)	Probability that the government organisation does not succeed in removing the relevant data in time or otherwise withdrawing it from the provider's access (prerequisite no. 7)	100%		100%	*Google has explained in the past 2 years it has not disclosed any Website Data belonging to public sector or education institutions located in the Netherlands in response to requests from law enforcement agencies (such as requests made under warrant or subpoena) based in Australia; Brazil; Chile; Hong Kong; India; Singapore; Taiwan; or the United States (US). However, Google does not disclose statistics about disclosure to security services/intelligence agencies. It is plausible that Google will be subjected to gagging orders from security services, and not permitted to inform its Customer. Hence Google may not be in a position to issue a timely warning to its customer. The probability is set to 100% absent an explanation from Google.*

Residual risk of successful lawful access by a foreign authority through the provider (given the countermeasures):	3,75%	Result of multiplication of E45*E46*E50*E51*E52*E53

Step 4b: Probability of foreign lawful access by mass surveillance of contents

Legal Basis considered for the following assessment: Unknown for Australia, Brazil, Chile, Hong Kong, India, Singapore and Taiwan, EU Adequacy Decision for the USA including FISA

		Probability in the period			Rationale
a)	Probability that the data at issue is transmitted to the provider or its subcontractors in a manner that permits the telecommunications providers in the country to view it in plain text as part of an upstream monitoring of Internet backbones	0%	0,00%	0,05%	*Google applies encryption in transit for inter-region data traffic and global routing (ALTS and TLS, plus the MTA-STS standard for mail), and AED for data stored at rest. Google also writes it never gives any government "backdoor" access." In reply to questions about access to encryption keys as part of 'backdoors', Google has further clarified: "Google will not disable security features or alter Meet systems to allow third parties to gain access to Customer Personal Data that would otherwise be unavailable to a third party in clear text."*
b)	Probability that the data transmitted will include content picked by	0%			*Idem.*
c)	Probability that the provider or a subcontractor in the country is technically able to on an ongoing basis search the data in plain text for selectors (i.e. search terms such certain recipients or senders of electronic communications) without the customer's permission as part of a downstream monitoring of online communications	10%	0,05%		*As Google applies the encryption, Google and its subsidiaries are technically capable of lifting that encryption, and can do so in practice for service maintenance, troubleshooting and technical support. The probability that Google performs such a search for an IP address or the unique cookie identifier from the NID-cookie cannot be excluded.*
d)	Probability that the provider or a subcontractor in the countries above may be legally required to perform such as search (also) with the company's data	1%			*Speculative estimate. This refers to Upstream Data Collection. According to the Adequacy Decision from the European Commission, personal data may be transferred to the USA without having to put additional measures in place, but no such analysis is available for the 7 third countries. It is plausible that some Website Data from a Dutch education organisation are interesting for security services in the 7 third countries where they may be accessed. This probability is low based on Google's statement that it has not provided any government with direct access to any information stored in its data centers, including data stored or processed by the Meet application (i.e. including direct access for security services).*
e)	Probability that the data is regarded as content that is the subject of intelligence searches in the country as per the above laws	50%			*It is plausible that Website Data from a Dutch education organisation are interesting for security services in the 7 third countries where they may be accessed. Since customers cannot encrypt Website Data with their own key, and they reveal the IP-address, as well as the unique identifier from the NID-cookie, the probability of interest in the personal data in Content Data is estimated to be 50% (similar to the Content, Account and Diagnostic Data).*

Residual risk of successful lawful access by a foreign intelligence service without any guarantee of legal recourse (in view of the countermeasures):	0,05%

Step 5: Overall assessment

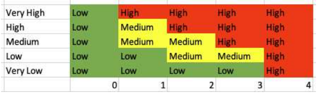
Probability that the question of lawful access via the cloud provider will arise at all (1 case in the period = 100%)	90,00%
Probability of successful lawful access by the foreign authorities concerned in these cases despite the countermeasures	3,75%
Probability of additional successful lawful access by a foreign intelligence service where there is no guarantee of legal recourse (despite countermeasures)	0,05%
Overall probability of a successful lawful access to data in plain text via the cloud provider in the observation period:	3,43%
Description in words (based on Hillson*):	Very low
The number of years it takes for a lawful access to occur at least once with a **90 percent** probability:	132
The number of years it takes for a lawful access to occur at least once with a **50 percent** probability:	40

... assuming that the probability neither increases nor decreases over time (like tossing a coin)

** Scale: <5% = "Very low", 5-10% = "Low", 11-25 = "Medium", 26-50% = "High" and >50% = "Very high" (by David Hillson, 2005, see https://www.pmi.org/learning/library/describing-probability-limitations-natural-language-7556).*

Step 6: Data subject risks

				Rationale
a)	*Estimated probability of occurrence of successful lawful access risk:*	*3,43%*	*Very Low*	
		1= pseudonymised regular personal data	*Low*	*The Website Data should only contain pseudonymised personal data (IP address, unique identifier in cookies and registered activities, such as participating via a browser in a Meet). The impact of unauthorised access to pseudonymised personal data is low. In view of the very low probability that the risk of unauthorised access materialise, the risk is assessed as low.* *Though there are no high risks anymore for the transfer to the USA, such guarantees are not available for transfer to Google's data centres in Australia; Brazil; Chile; Hong Kong; India; Singapore and Taiwan.*
b)	*Estimated impact of risk*			



Very High	Low	High	High	High	High
High	Low	Medium	High	High	High
Medium	Low	Medium	Medium	High	High
Low	Low	Low	Medium	Medium	High
Very Low	Low	Low	Low	Low	High
	0	1	2	3	4

Low

Step 7: Define the safeguards in place

				Rationale
a)	Would it be feasible, from a practical, technical and economical point of view, for the data exporter to transfer the personal data in question to a location in a whitelisted country instead?	Yes	*Describe why you still do not pursue this option*	*Google does not make a Data Region choice available for Website Data as part of the Service Data. Google has not disclosed any plans to limit access to Service Data to EU-based engineers only. This means the Website Data can be processed by support engineers in the USA, and in the 7 third countries.*
b)	Is the personal data transferred under one of the exemptions pursuant to applicable data protection law (e.g., Art. 49 GDPR in case of the GDPR)?	No		*Once an education organisation uses Google Meet, the transfer of Website Data is structural, not incidental.*
c)	Is the personal data at issue transmitted to the target jurisdiction in clear text (i.e. there is no appropriate encryption in-transit)?	No	*Ensure that data remains encrypted*	*No, Google by default applies encryption both in-transit and to stored data, but with its own keys. It is not possible to apply CSE to the Website Data.*
d)	Is the personal data at issue accessible in the target jurisdiction in clear text by the data importer/recipient or a third party (i.e. the data is either not appropriately encrypted or access to the keys to decrypt is possible)?	Yes	*Foreign lawful access is at least technically possible*	*Yes, Google and its subsidiaries in 3d countries can technically access the unencrypted Website Data, although this would be a violation of policy and organisational measures.*
e)	Is the personal data at issue protected by a transfer mechanism approved by the applicable data protection law (e.g., the EU Standard Contractual Clauses in case of the GDPR, approved BCR, or - in the case of an onward transfer - a back-to-back-contract in line with the EU SCCs), and can you expect compliance with it, insofar permitted by the target jurisdiction, and judicial enforcement (where applicable)?	Yes	*Ensure that the mechanism remains in place and is complied with*	*The Dutch education customers rely on appropriate transfer mechanisms under Chapter V GDPR.*

Based on the answers given above, the transfer is: permitted

Final Step: Conclusion

In view of the above and the applicable data protection laws, the transfer is: permitted

Reassess at the latest by: X+2
(or if there are any changes in circumstances)

This Transfer Impact Assessment has been made by:
SLM Rijk / SURF / SIVON / PRIVACY COMPANY

Place, Date:
Signed: ____________________
By: [School or University X]