Data Transfer Impact Assessment (DTIA) on the Customer Data includes the contents of information shared by customers as Support transfer to third countries of Content Data processed This DTIA was made by Privacy Company, and SLM Microsoft, Google and Amazon Web Services Rijk, using and adapting the template provided by David Rosenthal, provided under CC license 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 by Google Meet (audio/video conferencing) 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. COMMENTS GOOGLE OR PRIVACY COMPANY **Step 1: Describe the intended transfer** Dutch government organisation [X] a) Data exporter (or the sender in case of a relevant onward transfer): [Confidential] for the Dutch public 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 b) Country of data exporter: authorised. Google LLC in the USA. The Dutch public sector customers rely on appropriate transfer mechanisms under Chapter V GDPR. c) Data importer (or the recipient in case of a relevant onward transfer): USA, with onward transfers to third countries for recorded data. The contracting entity for Dutch public sector 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 d) Country of data importer: Cloud EMEA Limited is a wholly owned subsidiary of Google LLC, which in turn is a wholly owned subsidiary of Alphabet Inc. 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

Note Privacy Company: Google does not ask for specific consent for the transfer of video or just audio. The video conference service also offers related features such as text chatting and file sharing among participants, (Al generated) live captions. Content Data to employees in the first list of 12 third countries: the support 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. 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 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. assumes that government organisations will not provide such consent. 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, e) Context and purpose of the transfer: Singapore and Taiwan, plus the USA. rsonal 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 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 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 belonging to public sector institutions located in the Netherlands in the Google Workspace administrators and employee users of Dutch public sector organisations + external participants in Meet conferences (as guest users, or with a Google account). f) Categories of data subjects concerned: 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 g) Categories of personal data transferred: 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 h) Sensitive and special categories of personal data: 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. Google allows its Workspace Enterprise 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. public sector customers of the 'free' Workspace versions (for nonprofits or Enterprise Essential) 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 government organisations will select the EU as data region, and will not provide consent for such access if it i) Technical implementation of the transfer: 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 Enterprise customers with access controls to prevent access for support outside of the EU, processing-inregion 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. Privacy Company has tested the effectivity of CSE for Meet with a self-controlled 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 and Google's FlowCrypt keyserver, and third party (open source) identity provider, and warnings to end users that many desired functionalities won't work, this DTIA assumes that Dutch government organisations do no use CSE for day to day use. encountered some issues. Currently, admins cannot centrally enforce the use of CSE 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 for Meet, and the options for end users to enable CSE are hard to find. Google has 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. 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 Google has provided contractual guarantees to the Dutch public sector customers that sub-processors may only process personal data in accordance with the framework agreement, and that this guarantee applies to encryption prevents users from using the features recording, live streaming, 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 connecting with a phone, use of breakout rooms, host management, polls, Q&A, noise 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: cancellation, whiteboarding or transferring calls between Google Workspace apps. https://services.google.com/fh/files/misc/safeguards_for_international_data_transfers_with_google_cloud.pdf. Another identified issue is the impossibility to invite guest users without Google 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 account to use client-side encryption in a school-initiated Meet (for example, a parent access to a Google Drive folder with recorded Meets or transcripts. But the second category of Google and required. Google and required teacher meeting about the progress of a pupil). Google explains in the article about j) Technical and organizational measures in place: 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 CSE in Meet: The knocking capability to allow a guest is disabled. data, our account controls, our compliance audits, and our certifications. https://support.google.com/meet/answer/11605714?hl=en-GB). As part of the organisational measures Google offers results of audits through its Compliance reports or certificates are only accessible if the Additional Service Google Developers is Finally, admins must once use the Google Cloud to create an API-key (to allow the activated (which should be disabled), Google has clarified that Dutch public sector Workspace admins can request direct access to the SOC2 and BSI C5 audit reports through their account manager. external keyserver to talk to Google), a service that is outside the negotiated 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 Workspace contract because Google Cloud is an Additional Service in Workspace. 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: Google has assured that it is a processor for this limited use of the Google Cloud 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 Platform in this case, based on the GCP Terms of Service (which incorporate the 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 Cloud Processing Addendum). Google publishes separate transparency reports for compelled disclosure of data from Cloud and Workspace public sector 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 institutions located in the Netherlands during the past 2 years (the assessment period). 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 for Workspace Enterprise customers, 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. k) Relevant onward transfer(s) of personal data (if any): 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 Google has explained: "If customers wish to avoid the possibility that a listed technical 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 Subprocessor could access Customer Data or Service Data for technical 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. support purposes then they are not required to use technical support. Accordingly, I) Countries of recipients of relevant onward transfer(s): 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: 22 October 2024 b) Assessment period in years: c) Ending date of the assessment based on the above: Australia, Brasil, Chile, Hong Kong, India, Singapore and This includes access for technical support by engineers in these 7 third countries. It is assumed that Dutch public sector Workspace d) Target jurisdiction for which the DTIA is made: 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 Taiwan + United States request. e) Is importer an Electronic Communications Service Provider as Yes defined in USC § 1881(b)(4): Google explains in its "Government Requests for Cloud Customer Data" whitepaper that it commits to object to, or limit or modify, any f) Does importer/processor commit to legally resist every request for No 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 agreement with the Dutch government includes 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 government does not agree that Google is entitled to such voluntary disclosures. Google has assured the Dutch public sector that it has not disclosed any personal data from Dutch public sector customers in the past 2 years for this purpose. Google has not shared its legal analysis of applicable laws and their g) Relevant local laws taken into consideration: compliance with the fundamental right guarantees offered to data subjects in Australia, Brasil, Chile, Hong Kong, India, Singapore and Step 3: Probability that a foreign authority has a legal claim in the data and wishes to enforce it against the provider Probability Rationale Cases remaining per year per case In reply to this DTIA Google has stated it has not disclosed any Content Data from Dutch public sector customers to law enforcement in a) Number of cases under the laws listed in Step 2g per year in which 100% the past two years: "We can confirm that, in the past two years (which we understand to be your 'assessment period'), we have not an authority in the third countries is estimated to attempt to obtain disclosed any Customer Data or Service Data belonging belonging to public sector institutions located in the Netherlands in response to relevant data through <u>legal action</u> during the period under requests from law enforcement agencies (such as requests made under warrant or subpoena) based in Australia; Brazil; Chile; Hong Kong; consideration. India; Singapore; Taiwan; or the United States (US)." Google has also explicitly confirmed it has not voluntarily disclosed any personal data from Dutch public sector 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. 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 b) Share of such cases in which the request occurs in connection with a 100% countries are permitted to obtain data from Google. For example, as Hong Kong is part of China, governments across the EU have case that due to its nature in principle permits the authority to expressed concerns about access by Chinese authorities to personal data from EU citizens. As quoted above, though Google has not obtain the data also from a provider disclosed any Dutch public sector 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. According to Google, CSE is not necessary for day-to-day use. Google explains: "This additional control can help you strengthen the Probability that in the remaining such cases it will be possible for 10% confidentiality of your sensitive or regulated data. Your organization might need to use CSE for various reasons—for example: the company to successfully cause the authority (by legal means or Privacy—Your organization works with extremely sensitive intellectual property. otherwise) to give up its request for the data in plain text 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 government organisations 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. Absent an MLAT with the third country, EU organisations cannot consent to disclose Content Data to a government authority in a third d) Probability that in the remaining cases the requested data will be 1% country, based on Art 48 GDPR. Google has explained in reply to this DTIA that it has not provided any personal data from Dutch public provided in one way or another (e.g., with consent or through legal sector customers to law enforcement authorities in the assessment period, also not on a voluntary basis. or administrative assistance) e) Probability that in the remaining cases the authority will consider 50% 0,45 Enforcing lawful access via Google to access data of one of its public sector 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 the data it is seeking to be so important that it will look for another want to undergo such trouble only in particularly important cases, thus significantly reducing the number of relevant cases. way to obtain it Based on E35, which is a calculation of C35*D34. D34 is calculated as (1-C34)*D33 Number of cases per year in which the question of lawful access by a foreign authority arises Number of cases in the period under consideration 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 Google is a well-known cloud services provider with a substantial amount of public sector Workspace customers in the EU a) Probability that the authority is aware of the provider and its subcontractors (prerequisite no. 1) 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 Google has explained that the probability of access to specific content is very low, even b) Probability that an employee of the provider or its subcontractors 0% 0,00% of technical service maintenance and support, but they need to be authorised to access specific data [see below]. will gain access to the data in plain text in a support-case .. absent CSE. "For context, the nature of Google Meet is such that the Customer Data Government organisations cannot prevent access to the recorded Content Data by the support engineers in these 7 third countries if they that is 'generated' during a meeting is predominantly transient. For example, video (prerequisite no. 2) file a support request. They can only lower the probability of access for this purpose by never filing a support request with Google. and audio streams of a conversation between two Meet participants (e.g. a teacher 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 and student). Google support agents would have no reason to join such a meeting as customers can view the availability stats of Meet in the Netherlands to make an estimate of the probability of such transfers. These stats that would not be required for their role. Google Meet includes measures by default 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. 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)." Google employees can incidentally be tasked to look at problems from Dutch customers with Meet, but they cannot 'search' for any .. and is able to search for, find and copy the data requested by the 1% customers' personal data. Google explains: "Access is entirely dependent on the specific activity they need to perform and only occurs authority (prerequisite no. 3) 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." This DTIA assumes government organisations do not use CSE for day to day use. Though Google applies encryption to the data-at-rest, c) Probability that despite the technical countermeasures taken, 10% Google has access to the key, and can therefore (theoretically) decrypt these data if ordered to do so. Though Google has not provided any employees of the provider, of its subcontractors or of the parent personal data from Dutch public sector customers to law enforcement in the past 2 years, Google is prohibited from publishing details company technically have access to data in plain text (also) outside about disclosure to security services. a support situation (e.g., using admin privileges) or are able to gain 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 such access, e.g., by covertly installing a backdoor or "hacking" into has not joined any program that would give the U.S. government—or any other government—direct access to its servers." Google has the system (irrespective of whether they are allowed to do so) ... clarified that this statement also applies to indirect access through for example, distribution of a new version or temporary lifting of (prerequisite no. 2) 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 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. It is unlikely that Google employees in these third countries would succeed in gaining access and be able to search for the data specifically .. and are then able to search for, find and copy the data requested 1% requested by an authority. by the authority (prerequisite no. 3) Google explains in its information about subprocessors that its subsidiaries in the 7 third countries may have access to (recorded) Content d) Probability that the provider, the subcontractor or its parent 100% Data from Meet for the purposes of software and systems engineering, maintenance and troubleshooting. See: company, respectively, is located within the jurisdiction of the https://workspace.google.com/terms/subprocessors.html. authority (prerequisite no. 4) Speculative estimate. This DTIA assumes government organisations do not use CSE for day to day use. Though Google by default applies e) Probability that despite the technically limited access and the encryption to both streaming and recorded data, Google has access to these keys, can use these keys to decrypt if necessary for technical and organizational countermeasures in place, the troubleshooting, and can hence also be ordered to decrypt the data. Therefore the probability that government authorities in the 3d authority is permitted to order the provider, its subcontractor or the 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 parent company, respectively, to obtain access to the data and 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. produce it to the authority in plain text (prerequisite no. 5) Privacy Company has studied the confidential SOC-2 and C5:2020 audit reports. These reports do not note any deviations/findings with f) Probability that if data were to be handed over to the foreign 50% regard to transfers and disclosure of Content Data to third parties to fulfill requests. Additionally, Google has a Code of Conduct, in which authority, this would lead to the criminal liability of employees of it mentions the existence of anti-bribery laws, with the following sentence: "Like all businesses, Google is subject to lots of laws, both the provider or its subcontractors, the prosecution of which would U.S. and non-U.S., that prohibit bribery in virtually every kind of commercial setting." URL: https://abc.xyz/investor/google-code-ofbe possible and realistic, and as a consequence, the data does not 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 have to be produced or is not produced (prerequisite no. 6) third countries is unknown. Google has explained it has not disclosed any Content Data belonging belonging to public sector institutions located in the Netherlands in g) Probability that the government or public sector organisation does 50% response to requests from law enforcement agencies (such as requests made under warrant or subpoena) based in Australia; Brazil; Chile; not succeed in removing the relevant data in time or otherwise Hong Kong; India; Singapore; Taiwan; or the United States (US), nor voluntarily disclosed any data from Dutch government and public withdrawing it from the provider's access (prerequisite no. 7) sector 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 a 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. Government organisations can further lower this probability by not making any recordings of Meets or at least apply a very short retention period. Result of multiplication of E45*E46*E50*E51*E52*E53 Residual risk of successful lawful access by a foreign authority through the provider (given the countermeasures): 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 This DTIA assumes government organisations do not use CSE for day to day use. However, Google applies encryption in transit for intera) Probability that the data at issue is transmitted to the provider or its 0% 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 subcontractors in a manner that permits the telecommunications writes it never gives any government "backdoor" access." In reply to questions about access to encryption keys as part of 'backdoors', providers in the country to view it in plain text as part of an Google has further clarified: "Google will not disable security features or alter Meet systems to allow third parties to gain access to upstream monitoring of Internet backbones Customer Personal Data that would otherwise be unavailable to a third party in clear text." See the explanation in the row above.) Probability that the data transmitted will include content picked by 0% selectors (i.e., intelligence search terms such as specific recipients or senders of electronic communications) As Google applies the encryption, Google and its subsidiaries are technically capable of lifting that encryption, and can do so in practice 0,05% c) Probability that the provider or a subcontractor in the country is 10% for troubleshooting. The probability that Google performs such a search cannot be excluded, but in view of the access limitations for technically able to on an ongoing basis search the data in plain text engineers, the fact that usage logs are controlled and there are no findings of any non-conformity in the past 2 years, this probability is 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 Speculative estimate. This refers to Upstream Data Collection. According to the Adequacy Decision from the European Commission, d) Probability that the provider or a subcontractor in the countries 1% personal data may be transferred to companies in the USA certified under the DPF without having to put additional supplementary above may be legally required to perform such as search (also) with measures (as described by the European Court of Justice and in the recommendations from the EDPB) in place. However, this DTIA the company's data assesses the risks of disclosure by subprocessors in 7 third countries. 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). It is plausible that some Content Data from a Dutch public sector organisation are interesting for security services in the 7 third countries e) Probability that the data is regarded as content that is the subject of 50% where they may be accessed. This DTIA assumes government organisations will not deploy CSE for day to day use, and rely on the intelligence searches in the country as per the above laws encryption applied by Google. Because the majority of Meets will not be encrypted with a self-controlled key, the probability of interest in the personal data in Content Data is estimated to be 50%. The probability of interest may even increase if security services deploy quantum computing to decrypt data stored with Google's keys. 0,05% Residual risk of successful lawful access by a foreign intelligence service without any guarantee of legal recourse (in view of the Step 5: Overall assessment 89,10% Probability that the question of lawful access via the cloud provider will arise at all (1 case in the period = 100%) Probability of successful lawful access by the foreign authorities concerned in these cases despite the countermeasures 0,01% 0,05% Probability of additional successful lawful access by a foreign intelligence service where there is no guarantee of legal recourse (despite Overall probability of a successful lawful access to data in plain text via the cloud provider in the observation period: 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: 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 a) Estimated probability of occurrence of successful lawful access risk: 4= special categories of data in the clear High The recorded Content Data can include special categories of data. If government organisations do not use CSE for Meets in which special categories of data are processed, even though the factual probability of unlawful access is very low, the impact of such access to special categories of personal data in Content Data in plain text can be very high. Therefore, 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; b) Estimated impact of risk Chile; Hong Kong; India; Singapore and Taiwan. This DTIA does assume 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.

Note: this tab describes the transfer of **Content Data**. Google uses the term **Customer**

https://cloud.google.com/terms/data-processing-addendum. Google's category of

Data in its public data processing agreement for cloud services. URL:

Step 7: Define the safeguards in place

Google allows its Workspace Enterprise customers 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 for paid Workspace customers with access controls to prevent access for support Would it be feasible, from a practical, technical and economical 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-Describe why you still do not pursue this option a) point of view, for the data exporter to transfer the personal data in Yes 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 question to a location in a whitelisted country instead? 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/productannouncements/announcing-sovereign-controls-for-google-workspace. Even though the probability of access by tech engineers in third countries to the data stored in the EU is very small, once a public sector Is the personal data transferred under one of the exemptions organisation uses Google Meet the transfer is structural, not incidental. b) pursuant to applicable data protection law (e.g., Art. 49 GDPR in case No of the GDPR)? No, Google by default applies encryption both in-transit and to stored data, but with its own keys. Customers can deploy CSE with their c) Is the personal data at issue transmitted to the target jurisdiction in clear text (i.e. there is no appropriate encryption in-transit)? Ensure that data remains own key server, but Google does not recommend this for daily use. This DTIA assumes that government organisations do not use CSE for encrypted day to day use. As explained in row 96 above, this DTIA assumes government organisations 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 Is the personal data at issue accessible in the target jurisdiction in violation of policy and organisational measures. d) 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 Foreign lawful access is at least technically possible decrypt is possible)? Is the personal data at issue protected by a transfer mechanism The Dutch public sector Enterprise customers can rely on appropriate transfer mechanisms under Chapter V GDPR. approved by the applicable data protection law (e.g., the EU

Standard Contractual Clauses in case of the GDPR, approved BCR, or - Yes in the case of an onward transfer - a back-to-back-contract in line Ensure that the mechanism remains in place and is complied with the EU SCCs), and can you expect compliance with it, insofar permitted by the target jurisdiction. and judicial enforcement Based on the answers given above, the transfer of sensitive and special categories of data without CSE is: 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: In view of the above and the applicable data protection laws, the transfer permitted

of regular personal data is:

SLM Microsoft, Google Cloud and Amazon Web Services Rijk / PRIVACY COMPANY

This Transfer Impact Assessment has been made by:

Dutch government organisation [X]

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

a) Data exporter (or the sender in case of a relevant onward transfer):

Very Low Low Low Low

Step 7: Define the safeguards in place

0 1 2 3 4

Step 1: Describe the intended transfer

This DTIA was made by Privacy Company, and SLM Microsoft, Google and Amazon Web Services Rijk, using and adapting the template provided by David Rosenthal, provided under CC license

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.

COMMENTS GOOGLE

[Confidential] for the Dutch public 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. b) Country of data exporter: Google LLC in the USA. The Dutch public sector customers rely on appropriate transfer mechanisms under Chapter V GDPR. c) Data importer (or the recipient in case of a relevant onward transfer): USA, with onward transfers to third countries for recorded data. The contracting entity for Dutch public sector 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 d) Country of data importer: Limited is a wholly owned subsidiary of Google LLC, which in turn is a wholly owned subsidiary of Alphabet Inc. 2 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 Google has not answered the question if Google Account Data from guest users in meetings 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. organised by public sector customers are offered the same processing guarantees. This DTIA This tab is about the transfer of the Account Data. assumes there is no such protection umbrella. 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 Note Privacy Company: Google does not ask for specific consent for the transfer of Account 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. Data (as part of Google's category of Service Data) to employees in the first list of 12 third 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 Drive folder). In that case, the Account countries: the support employees only asks for consent to access to Content or Service Data 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. of the customer without informing the customer in what country they operate. That is why e) Context and purpose of the transfer: 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 this DTIA assumes that government organisations will not provide such consent. 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 Account 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 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 belonging to public sector institutions located in the Netherlands in the past two years." Google Workspace administrators and employee users of Dutch public sector organisations + external participants in Meet conferences (as guest users, or with a Google account). f) Categories of data subjects concerned: 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 g) Categories of personal data transferred: necessary if the school or government organisation has chosen the 'Trusted' or 'Restricted' setting (not the 'Open' access setting). Account Data from admins and employees can be sensitive data, 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, and does h) Sensitive and special categories of personal data: not equal the legal definition of special categories of data. 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 i) Technical implementation of the transfer: 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. **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 public sectoral institution are not covered by the additional data protection measures such as Sovereign Controls. Organisational measures: Google has provided contractual guarantees to the Dutch public sector 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 and Service Data (including 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 j) Technical and organizational measures in place: 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 public sector 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 public sector institutions located in the Netherlands during the past 2 years (the assessment period). Account Data from Meet may be onward transferred to 7 third countries for software and systems engineering, maintenance and troubleshooting, and for technical support. k) Relevant onward transfer(s) of personal data (if any): 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 l) Countries of recipients of relevant onward transfer(s): 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 22 October 2024] b) Assessment period in years: c) Ending date of the assessment based on the above: This includes access for technical support by engineers in these 7 third countries. It is assumed that Dutch public sector Workspace Australia, Brasil, Chile, Hong Kong, India, Singapore and Taiwan + d) Target jurisdiction for which the DTIA is made: customers will not consent to the transfer of Account Data to the other list of subprocessors in 12 third countries in the context of a support **United States** e) Is importer an Electronic Communications Service Provider as defined in Yes USC § 1881(b)(4): Google explains in its "Government Requests for Cloud Customer Data" whitepaper that it commits to object to, or limit or modify, any f) Does importer/processor commit to legally resist every request for No 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 agreement with the Dutch government includes 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 government does not agree that Google is entitled to such voluntary disclosures. Google has assured the Dutch public sector that it has not disclosed any personal data from Dutch public sector customers in the past 2 years for this purpose. Google has not shared its legal analysis of applicable laws and their This DTIA cannot provide a detailed legal analysis of the applicable surveillance laws in the 7 third countries. Absent such an analysis, it g) Relevant local laws taken into consideration: has to be assumed that some or all authorities in the third countries are permitted to obtain data from Google. compliance with the fundamental right guarantees offered to data subjects 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 in Australia, Brasil, Chile, Hong Kong, India, Singapore and Taiwan. 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 Cases Probability Cases remaining per year per case 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 a) Number of cases under the laws listed in Step 2g per year in which an 100% 1,00 public sector customers to law enforcement in the past two years: "We can confirm that, in the past two years (which we understand to be authority in the third countries is estimated to attempt to obtain relevant your 'assessment period'), we have not disclosed any Customer Data or Service Data belonging belonging to public sector institutions data through <u>legal action</u> during the period under consideration. 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 public sector 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 100% 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 1,00 are permitted to obtain data from Google. For example, as Hong Kong is part of China, governments across the EU have recently expressed that due to its nature in principle permits the authority to obtain the data concerns about access by Chinese authorities to personal data from EU citizens. As quoted above, though Google has not disclosed any Dutch public sector 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. 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. c) Probability that in the remaining such cases it will be possible for the 0% company to successfully cause the authority (by legal means or otherwise) to give up its request for the data in plain text Absent an MLAT with the third country, EU organisations cannot consent to disclose Account Data to a government authority in a third d) Probability that in the remaining cases the requested data will be country, based on Art 48 GDPR. Google has explained in reply to this DTIA that it has not provided any personal data from Dutch public provided in one way or another (e.g., with consent or through legal or sector customers to law enforcement authorities in the assessment period, also not on a voluntary basis. administrative assistance) Enforcing lawful access via Google to access Account Data of one of its public sector customers (where it is a processor) is much more e) Probability that in the remaining cases the authority will consider the data 50% 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 it is seeking to be so important that it will look for another way to obtain will want to undergo such trouble only in particularly important cases, thus significantly reducing the number of relevant cases. 0,50 Based on E35, which is a calculation of C35*D34. D34 is calculated as (1-C34)*D33 Number of cases per year in which the question of lawful access by a foreign authority arises 0,99 Number of cases in the period under consideration 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 Google is a well-known cloud services provider with a substantial amount of public sector Workspace customers in the EU a) Probability that the authority is aware of the provider and its subcontractors (prerequisite no. 1) 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 0,00% b) Probability that an employee of the provider or its subcontractors will gain 0% technical service maintenance and support, but they need to be authorised to access specific data [see below]. access to the data in plain text in a support-case .. (prerequisite no. 2) Government organisations 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. Google employees can incidentally be tasked to look at problems from Dutch customers with Meet, but they cannot 'search' for any .. and is able to search for, find and copy the data requested by the customers' personal data. Google explains: "Access is entirely dependent on the specific activity they need to perform and only occurs authority (prerequisite no. 3) 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 [including the Account Data, comment added by Privacy Company] 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." 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 c) Probability that despite the technical countermeasures taken, employees 10% 5,00% (theoretically) decrypt these data if ordered to do so. Though Google has not provided any personal data from Dutch public sector of the provider, of its subcontractors or of the parent company technically customers to law enforcement in the past 2 years, Google is prohibited from publishing details about disclosure to security services. have access to data in plain text (also) outside a support situation (e.g., In reply to this DTIA Google has explained it has not built in any backdoors. "Google has not provided any government with direct access using admin privileges) or are able to gain such access, e.g., by covertly 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 installing a backdoor or "hacking" into the system (irrespective of whether has clarified that this statement also applies to indirect access through for example, distribution of a new version or temporary lifting of they are allowed to do so) ... (prerequisite no. 2) 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. 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 .. and are then able to search for, find and copy the data requested by the 50% Account Data specifically requested by an authority. authority (prerequisite no. 3) Google explains in its information about subprocessors that its subsidiaries in 7 third countries may have access to Account Data (as part d) Probability that the provider, the subcontractor or its parent company, 100% 100% of Service Data) for the purposes of software and systems engineering, maintenance and troubleshooting. See: respectively, is located within the jurisdiction of the authority (prerequisite no. https://workspace.google.com/terms/subprocessors.html 100% Speculative estimate. Though Google by default applies encryption to data-at-rest, including Account Data, Google has access to these e) Probability that despite the technically limited access and the technical 100% keys, can use these keys to decrypt if necessary for troubleshooting, and can hence also be ordered to decrypt the data. Therefore the and organizational countermeasures in place, the authority is permitted to probability that government authorities in the third countries can order Google to provide access to the Account Data is set to 100%. [Note: order the provider, its subcontractor or the parent company, respectively, the difference with Content Data is that not all Meets are recorded, and only retained for a short period of time]. to obtain access to the data and produce it to the authority in plain text Privacy Company has studied the confidential SOC-2 and C5:2020 audit reports. These reports do not note any deviations/findings with Probability that if data were to be handed over to the foreign authority, 50% regard to transfers and disclosure of Content Data (including the Account Data) to third parties to fulfill requests. The audit reports do not this would lead to the criminal liability of employees of the provider or its cover the usage of Diagnostic Data, while Account Data are also registered in telemetry data and in the audit logs. Google has a Code of subcontractors, the prosecution of which would be possible and realistic, Conduct, in which it mentions the existence of anti-bribery laws, with the following sentence: "Like all businesses, Google is subject to lots and as a consequence, the data does not have to be produced or is not of laws, both U.S. and non-U.S., that prohibit bribery in virtually every kind of commercial setting." URL: https://abc.xyz/investor/googleproduced (prerequisite no. 6) 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. Google has explained it has not disclosed any Account Data belonging belonging to public sector institutions located in the Netherlands in Probability that the government organisation does not succeed in response to requests from law enforcement agencies (such as requests made under warrant or subpoena) based in Australia; Brazil; Chile; removing the relevant data in time or otherwise withdrawing it from the Hong Kong; India; Singapore; Taiwan; or the United States (US), nor voluntarily disclosed any data from Dutch government and public provider's access (prerequisite no. 7) sector 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. 2,50% Residual risk of successful lawful access by a foreign authority through the provider (given the countermeasures): 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 a) Probability that the data at issue is transmitted to the provider or its 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 subcontractors in a manner that permits the telecommunications encryption keys as part of 'backdoors', Google has further clarified: "Google will not disable security features or alter Meet systems to allow providers in the country to view it in plain text as part of an upstream third parties to gain access to Customer Personal Data that would otherwise be unavailable to a third party in clear text." monitoring of Internet backbones See the explanation in the row above. b) Probability that the data transmitted will include content picked by 0% selectors (i.e., intelligence search terms such as specific recipients or senders of electronic communications) As Google applies the encryption, Google and its subsidiaries are technically capable of lifting that encryption, and can do so in practice for c) Probability that the provider or a subcontractor in the country is 0,05% troubleshooting. The probability that Google performs such a search cannot be excluded, but in view of the access limitations for technically able to on an ongoing basis search the data in plain text for engineers, the fact that usage logs are controlled and there are no findings of any non-conformity in the past 2 years, this probability is 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 Speculative estimate. This row refers to Upstream Data Collection. According to the Adequacy Decision from the European Commission, d) Probability that the provider or a subcontractor in the countries above may 1% personal data may be transferred to companies in the USA certified under the DPF without having to put additional supplementary be legally required to perform such as search (also) with the company's 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 50% It is plausible that some Account Data from a Dutch public sector organisation are interesting for security services in the 7 third countries where they may be accessed. Government organisations must rely on the encryption applied by Google. These data are more likely to be intelligence searches in the country as per the above laws 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. 0,05% Residual risk of successful lawful access by a foreign intelligence service without any guarantee of legal recourse (in view of the countermeasures): **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: Description in words (based on Hillson*): The number of years it takes for a lawful access to occur at least once with a **90 percent** probability: The number of years it takes for a lawful access to occur at least once with a **50 percent** probability: ... 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** a) Estimated probability of occurrence of successful lawful access risk: Very Low 3= regular personal data in the clear Even though Account Data can include sensitive data, for this assessment it is assumed organisations will follow the recommendation to use pseudonyms for such sspecific employees. Hence, the Account Data are regular personal data. The impact of the risk of access to these personal data is high, but the probability is very low. Therefore, the risk is low. Though there are no high risks anymore for the b) Estimated impact of risk 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. Low Low Medium Medium High

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 a public sector 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)?	teenmeany 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 public sector Enterprise customers can rely on appropriate transfer mechanisms under Chapter V GDPR.
Base	ed on the answers given above, the transfer is:	permitted	
Fina	ll Step: Conclusion		
	ew of the above and the applicable data protection laws, the transfer is	permitted	Reassess at the latest by: X+2
	Transfer Impact Assessment has been made by: Microsoft, Google Cloud and Amazon Web Services Rijk / PRIVACY COMPANY	Place, Date Signed By	

This tab describes the transfers of **Support Data**. Google considers Support Data a subsection of **Service Data**. This DTIA distinguishes between 5 categories of Service Data: data about support tickets, Account Data Transfer Impact Assessment (DTIA) on the Data, Diagnostic Data, Security Data and Website Data. Support Data do not include the contents of support tickets: as those are part of Google's category of **Customer Data**, described in this DTIA as transfer to third countries of Content Data processed This DTIA was made by Privacy Company, and SLM Microsoft, Google and Amazon Web Services Rijk, using and adapting the template provided by David Rosenthal, provided under CC license Content Data. Because there are differences in both the impact and the probability of unauthorised by Google Meet (audio/video conferencing) 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 **Step 1: Describe the intended transfer COMMENTS GOOGLE** [Confidential] for the Dutch public sector. Technically, Google maintains servers around the world and its support and service engineers in the 7 b) Country of data exporter: third countries can access data anywhere, if necessary and authorised. Google LLC in the USA. The Dutch public sector customers rely on appropriate transfer mechanisms under Chapter V GDPR. c) Data importer (or the recipient in case of a relevant onward transfer): USA, with onward transfers to third countries for recorded data. The contracting entity for Dutch public sector customers of Google Workspace is **Google Cloud EMEA Limited** (see https://cloud.google.com/terms/google-entity), a Google entity based in Dublin, Ireland. d) Country of data importer: Google Cloud EMEA Limited is a wholly owned subsidiary of Google LLC, which in turn is a wholly owned subsidiary of Alphabet Inc.

Output

Description: 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

Note Privacy Company: Google does not ask for specific consent for the transfer of Content Data to 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 live 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 This tab is about the access to support tickets by google engineers in third countries, including attachments sent by customers. operate. That is why this DTIA assumes that government organisations will not provide such consent. 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 public sector 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 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". e) Context and purpose of the transfer: 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 Support 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 it 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-initated 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 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 helonging helonging to public sector institutions located in the Netherlands in the past two years " Google Workspace administrators and employee users of Dutch public sector organisations + external participants in Meet conferences (as guest users, or with a Google account). f) Categories of data subjects concerned: 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 government organisations will follow the g) Categories of personal data transferred: recommendation from the DPIA not to upload any sensitive data as part of a support ticket. Support Data may include Account Data from admins and employees whose identity should remain confidential, and snippets of Content Data from confidential Meets. These data are 'sensitive' due to their impact on data subjects in case of unauthorised access. The term sensitive data relates to the impact on data subjects if there is unauthorised access to their data, and does not equal the legal definition of h) Sensitive and special categories of personal data: special categories of data. This DTIA assumes government organisations will follow the recommendation from the DPIA to pseudonymise account names of sspecific employees that incur high risks if their Google does not offer an option to Workspace public sector 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 government organisations 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 i) Technical implementation of the transfer: 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 Enterprise customers 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. 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 **●** 🖾 rdholder data **●** 🔀 nfi dential business data j) Technical and organizational measures in place: ● Parsonal 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. 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 k) Relevant onward transfer(s) of personal data (if any): involves transfer to 3d countries. 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 l) Countries of recipients of relevant onward transfer(s): 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 [assessment made on 22 October 2024] a) Starting date of the transfer: b) Assessment period in years: c) Ending date of the assessment based on the above: This includes access for technical support by engineers in these 7 third countries. It is assumed that Dutch public sector Workspace d) Target jurisdiction for which the DTIA is made: Australia, Brasil, Chile, Hong Kong, India, Singapore and customers will not consent to transfer of Account Data to the other list of subprocessors in 12 third countries in the context of a Taiwan + United States support request. e) Is importer an Electronic Communications Service Provider as Yes defined in USC § 1881(b)(4): Google explains in its "Government Requests for Cloud Customer Data" whitepaper that it commits to object to, or limit or f) Does importer/processor commit to legally resist every request for No modify, any legal process that it reasonably determines to be overbroad, disproportionate, incompatible with applicable law, or access: otherwise unlawful. See Step 2 on page 7. The confidential agreement with the Dutch government includes 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 government does not agree that Google is entitled to such voluntary disclosures. Google has assured the Dutch public sector that it has not disclosed any personal data from Dutch public sector customers in the past 2 years for this purpose. This DTIA cannot provide a detailed legal analysis of the applicable surveillance laws in the 7 third countries. Absent such an Google has not shared its legal analysis of applicable laws and their g) Relevant local laws taken into consideration: analysis, it has to be assumed that some or all authorities in the third countries are permitted to obtain data from Google. compliance with the fundamental right guarantees offered to data Since the adequacy decision for the USA from the European Commission on 10 July 2023, transfers to the USA based on the DPF do subjects in Australia, Brasil, Chile, Hong Kong, India, Singapore and 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 remaining per case per year a) Number of cases under the laws listed in Step 2g per year in which 100% In reply to this DTIA Google has stated it has not disclosed any Support Data (as part of Service Data) from Dutch public sector customers to law enforcement in the past two years: "We can confirm that, in the past two years (which we understand to be an authority in the third countries is estimated to attempt to obtain your 'assessment period'), we have not disclosed any Customer Data or Service Data belonging belonging to public sector relevant data through <u>legal action</u> during the period under institutions located in the Netherlands in response to requests from law enforcement agencies (such as requests made under consideration. 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 public sector 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 100% 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 case that due to its nature in principle permits the authority to expressed concerns about access by Chinese authorities to personal data from EU citizens. As quoted above, though Google has obtain the data also from a provider not disclosed any Dutch public sector Support Data to law enforcement authorities in these countries in the past 2 years, disclosure to intelligence/security services cannot be excluded. CSE is not available for Support Data. Therefore, the probability that Google is not able to produce the Account Data in clear text, is c) Probability that in the remaining such cases it will be possible for 0% the company to successfully cause the authority (by legal means or otherwise) to give up its request for the data in plain text Absent a MLAT with the third country, EU organisations cannot consent to disclose Support Data to a government authority in a d) Probability that in the remaining cases the requested data will be 1% third country, based on Art 48 GDPR. Google has explained in reply to this DTIA that it has not provided any personal data from provided in one way or another (e.g., with consent or through legal Dutch public sector customers to law enforcement authorities in the assessment period, also not on a voluntary basis. or administrative assistance) Enforcing lawful access via Google to access Support data of one of its public sector customers (where it is a processor) is much e) Probability that in the remaining cases the authority will consider 10% more difficult than in the case of data of private individuals (where it is a controller). As Support Data only cover limited datasets, the data it is seeking to be so important that it will look for another the likelihood is much lower than requests for Content or Account Data. Therefore, we believe that the authorities will want to way to obtain it 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 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 Based on E37*C21 Step 4a: Probability that a foreign authority will successfully enforce the claim through the provider Unknown for Australia, Brasil, Chile, Hong Kong, India, Singapore and Taiwan, EU Adequacy Decision for registered participants in the EU-US Data Privacy Framework Legal Basis considered for the following assessment: Prerequisite for success Probability per case Google is a well-known cloud services provider with a substantial amount of public sector Workspace customers in the EU a) Probability that the authority is aware of the provider and its subcontractors (prerequisite no. 1) Customers can intentionally, with consent, allow Google support employees in 12 third countries to access Account Data in plain b) Probability that an employee of the provider or its subcontractors 0% 0,00% text as part of a support request. It is assumed that Dutch public sector Workspace customers will not consent to such a transfer. will gain access to the data in plain text in a support-case .. However, the Support Data can also be accessed without such consent by subprocessors in Australia, Brasil, Chile, Hong Kong, (prerequisite no. 2) specific data [see below]. Government organisations 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. Google employees can incidentally be tasked to look at problems from Dutch customers with Meet, but they cannot 'search' for .. and is able to search for, find and copy the data requested by the 1% any customers' personal data. Google explains: "Access is entirely dependent on the specific activity they need to perform and only authority (prerequisite no. 3) 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." Though Google applies encryption to the data-at-rest, Google has access to the key, and can therefore (theoretically) decrypt these c) Probability that despite the technical countermeasures taken, 10% data if ordered to do so. Though Google has not provided any personal data from Dutch public sector customers to law employees of the provider, of its subcontractors or of the parent enforcement in the past 2 years, Google is prohibited from publishing details about disclosure to security services. company technically have access to data in plain text (also) outside In reply to this DTIA Google has explained it has not built in any backdoors. "Google has not provided any government with direct a support situation (e.g., using admin privileges) or are able to gain 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 such access, e.g., by covertly installing a backdoor or "hacking" into servers." Google has clarified that this statement also applies to indirect access through for example, distribution of a new version the system (irrespective of whether they are allowed to do so) ... or temporary lifting of transit encryption. "Google will not disable security features or alter Meet systems to allow third parties to (prerequisite no. 2) 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 It is not plausible that Google would succeed in finding the data specifically requested by an authority in the Support Tickets .. and are then able to search for, find and copy the data requested 10% (different from Content, Diagnostic and Account Data). by the authority (prerequisite no. 3) Google explains in its information about subprocessors that its subsidiaries in 7 third countries may have access to Support Data d) Probability that the provider, the subcontractor or its parent 100% from Meet for the purposes of software and systems engineering, maintenance and troubleshooting, and for technical support. company, respectively, is located within the jurisdiction of the See: https://workspace.google.com/terms/subprocessors.html authority (prerequisite no. 4) Though Google by default applies encryption to data-at-rest, including Support Data, Google has access to these keys, can use e) Probability that despite the technically limited access and the 100% these keys to decrypt if necessary for troubleshooting, and can hence also be ordered to decrypt the data. Therefore the probability technical and organizational countermeasures in place, the that government authorities in the third countries can order Google to provide access to the Support Data is 100% (even if the authority is permitted to order the provider, its subcontractor or the chance that the requested data are available regaring a specific customer is very low). parent company, respectively, to obtain access to the data and produce it to the authority in plain text (prerequisite no. 5) Privacy Company has studied the confidential SOC-2 and C5:2020 audit reports. These reports do not note any deviations/findings Probability that if data were to be handed over to the foreign 50% with regard to transfers and disclosure of Content Data to third parties to fulfill requests. The audit reports do not cover the usage authority, this would lead to the criminal liability of employees of of Diagnostic Data, while Support Data may include Account Data, Telemetry Data and data from audit logs. Google has a Code of the provider or its subcontractors, the prosecution of which would Conduct, in which it mentions the existence of anti-bribery laws, with the following sentence: "Like all businesses, Google is be possible and realistic, and as a consequence, the data does not 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/ have to be produced or is not produced (prerequisite no. 6) 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. Google has explained it has not disclosed any Support Data belonging belonging to public sector institutions located in the Probability that the government organisation does not succeed in 100% Netherlands in response to requests from law enforcement agencies (such as requests made under warrant or subpoena) based in removing the relevant data in time or otherwise withdrawing it Australia; Brazil; Chile; Hong Kong; India; Singapore; Taiwan; or the United States (US), nor voluntarily disclosed any data from from the provider's access (prerequisite no. 7) Dutch government and public sector 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. 0,50% Result of multiplication of E45*E46*E50*E51*E52*E53 Residual risk of successful lawful access by a foreign authority through the provider (given the countermeasures): Step 4b: Probability of foreign lawful access by mass surveillance of contents 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 Legal Basis considered for the following assessment: Google applies encryption in transit for inter-region data traffic and global routing (ALTS and TLS, plus the MTA-STS standard for a) Probability that the data at issue is transmitted to the provider or its 0% mail), and AED for data stored at rest. Google also writes it never gives any government "backdoor" access." In reply to questions subcontractors in a manner that permits the telecommunications about access to encryption keys as part of 'backdoors', Google has further clarified: "Google will not disable security features or providers in the country to view it in plain text as part of an upstream monitoring of Internet backbones party in clear text." See the explanation in the row above. b) Probability that the data transmitted will include content picked by 0% selectors (i.e., intelligence search terms such as specific recipients or senders of electronic communications) As Google applies the encryption to the data-at-rest (in filed support tickets), Google and its subsidiaries are technically capable of c) Probability that the provider or a subcontractor in the country is 10% 0,01% lifting that encryption, and can do so in practice for troubleshooting. Because the support metadata such as names of participants technically able to on an ongoing basis search the data in plain text cannot be encrypted with CSE, the probability that a Google subsidiary is ordered to perform such a search cannot be excluded. 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 Speculative estimate. This refers to Upstream Data Collection. According to the Adequacy Decision from the European d) Probability that the provider or a subcontractor in the countries 1% Commission, personal data may be transferred to companies in the USA certified under the DPF without having to put additional above may be legally required to perform such as search (also) with supplementary measures (as described by the European Court of Justice and in the recommendations from the EDPB) in place. the company's data It is plausible that some Support Data (metadata) 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). It is possible, but not likely that some Support Data from a Dutch public sector organisation are interesting for security services in e) Probability that the data is regarded as content that is the subject of 10% the 7 third countries where they may be accessed. Since the metadata may include Meet names and account names, and intelligence searches in the country as per the above laws customers cannot encrypt the Support metadata with their own key, interest cannot be excluded. However, as 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 0,01% countermeasures): 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% 0,50% 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 Overall probability of a successful lawful access to data in plain text via the cloud provider in the observation period: Description in words (based on Hillson*): 4.222 The number of years it takes for a lawful access to occur at least once with a **90 percent** probability: 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 a) Estimated probability of occurrence of successful lawful access risk: 0,11% Very Low 3= regular personal data in the clear High This assessment assumes organisations will follow the recommendation to use pseudonyms for sspecific employees 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 is low. The probability that the risk of unauthorised b) Estimated impact of risk access occurs, is very low. Hence the risk is assessed as low. Step 7: Define the safeguards in place 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 Would it be feasible, from a practical, technical and economical Service Data. Google has not disclosed any plans to limit this access to EU-based engineers only. This means the Support Data can Describe why you still do not a) point of view, for the data exporter to transfer the personal data in Yes be processed by support engineers in the USA, and in the 7 third countries. pursue this option question to a location in a whitelisted country instead? Even though the probability of access by tech engineers in third countries to the Support Data is very small, once a public sector Is the personal data transferred under one of the exemptions organisation uses Google Meet the transfer is structural, not incidental. b) pursuant to applicable data protection law (e.g., Art. 49 GDPR in case No Is the personal data at issue transmitted to the target jurisdiction in Ensure that data remains 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 clear text (i.e. there is no appropriate encryption in-transit)? encrypted the Support Data. 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. 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 Foreign lawful access is at least data is either not appropriately encrypted or access to the keys to technically possible decrypt is possible)? The Dutch public sector Enterprise customers can rely on appropriate transfer mechanisms under Chapter V GDPR. Is the personal data at issue protected by a transfer mechanism approved by the applicable data protection law (e.g., the EU Ensure that the mechanism Standard Contractual Clauses in case of the GDPR, approved BCR, or remains in place and is complied 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

Based on the answers given above, the transfer is:

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

Reassess at the latest by: X+2

This Transfer Impact Assessment has been made by:

SLM Microsoft, Google Cloud and Amazon Web Services Rijk / PRIVACY COMPANY

Signed:

Data Transfer Impact Assessment (DTIA) on the Diagnostic Data a subsection of **Service Data**. This DTIA distinguishes between 5 categories of Service Data: data about support tickets, Account Data, Diagnostic Data, transfer to third countries of Content Data processed This DTIA was made by Privacy Company, and SLM Microsoft, Google and Amazon Web Services Rijk, using and adapting the template provided by David Rosenthal, provided under CC license Security Data and Website Data. Because there are differences in both the impact and by Google Meet (audio/video conferencing) 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 government organisation [X] [Confidential] for the Dutch public 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 b) Country of data exporter: authorised. Google LLC in the USA. The Dutch public sector customers rely on appropriate transfer mechanisms under Chapter V GDPR. c) Data importer (or the recipient in case of a relevant onward transfer): USA, with onward transfers to third countries for recorded data. The contracting entity for Dutch public sector 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 d) Country of data importer: Cloud EMEA Limited is a wholly owned subsidiary of Google LLC, which in turn is a wholly owned subsidiary of Alphabet Inc. 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 Note Privacy Company: Google does not ask for specific consent for the transfer of video or just audio. The video conference service also offers related features such as text chatting and file sharing among participants, (Al generated) live captions. Content Data to employees in the first list of 12 third countries: the support 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 employees only ask for consent to access Content or Service Data of the customer of a Meet (as observed to be part of Telemetry Data). This tab does not include the specific webserver access by guest users, end-users and admins to without informing the customer in what country they operate. That is why this DTIA 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. assumes that Dutch government organisations will not provide such consent. 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 public sector 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 e) Context and purpose of the transfer: 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 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 belonging to public sector institutions located in the Netherlands in the Google Workspace administrators, employee users of Dutch public sector organisations + external participants in Meet conferences (as guest users, or with a Google account). f) Categories of data subjects concerned: 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 sspecific employees. 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 g) Categories of personal data transferred: users cannot be pseudonymised and (2) frequent Meets in a short period of time between different government security officers may reveal cyber incidents. See row 10. h) Sensitive and special categories of personal data: 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. i) Technical implementation of the transfer: This means the Service Data may be transferred to the 7 third countries as well as the USA where Google processes Service Data. 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 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 j) Technical and organizational measures in place: 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): <u>Diagnostic Data</u> 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 22 October 2024] b) Assessment period in years: c) Ending date of the assessment based on the above: d) Target jurisdiction for which the DTIA is made: This includes access to Service Data for service maintenance and for technical support by engineers in these 7 third countries. It is Australia, Brasil, Chile, Hong Kong, India, Singapore and assumed that Dutch public sector Workspace customers will not consent to transfer of Service Data to the other list of subprocessors in Taiwan + United States 12 third countries in the context of a support request. e) Is importer an Electronic Communications Service Provider as Yes defined in USC § 1881(b)(4): Google explains in its "Government Requests for Cloud Customer Data" whitepaper that it commits to object to, or limit or modify, any f) Does importer/processor commit to legally resist every request for No legal process that it reasonably determines to be overbroad, disproportionate, incompatible with applicable law, or otherwise unlawful. access: See Step 2 on page 7. However, this guide does not cover the Service Data. The confidential agreement with the Dutch government includes 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 government does not agree that Google is entitled to such voluntary disclosures. Google has assured the Dutch public sector that it has not disclosed any personal data from Dutch public sector customers in the past 2 years for this purpose. This DTIA cannot provide a detailed legal analysis of the applicable surveillance laws in the 7 third countries. Absent such an analysis, it Google has not shared its legal analysis of applicable laws and their g) Relevant local laws taken into consideration: has to be assumed that some or all authorities in the third countries are permitted to obtain data from Google. compliance with the fundamental right guarantees offered to data 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 subjects in Australia, Brasil, Chile, Hong Kong, India, Singapore and 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 Cases remaining per year In reply to this DTIA Google has stated it has not disclosed any Diagnostic Data (as part of Service Data) from Dutch public sector a) Number of cases under the laws listed in Step 2g per year in which 100% customers to law enforcement in the past two years: "We can confirm that, in the past two years (which we understand to be your an authority in the third countries is estimated to attempt to obtain 'assessment period'), we have not disclosed any Customer Data or Service Data belonging to Education or public sector institutions relevant data through <u>legal action</u> during the period under located in the Netherlands in response to requests from law enforcement agencies (such as requests made under warrant or subpoena) consideration. 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 public sector 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-nationalsecurity. 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. 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 b) Share of such cases in which the request occurs in connection with a 100% countries are permitted to obtain data from Google. For example, as Hong Kong is part of China, governments across the EU have case that due to its nature in principle permits the authority to expressed concerns about access by Chinese authorities to personal data from EU citizens. As quoted above, though Google has not obtain the data also from a provider disclosed any Dutch public sector 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. CSE is not available for Diagnostic Data. Therefore, the probability that Google is not able to produce these data in clear text, is zero. Probability that in the remaining such cases it will be possible for 0% the company to successfully cause the authority (by legal means or otherwise) to give up its request for the data in plain text Absent a MLAT with the third country, EU organisations cannot consent to disclose Diagnostic Data to a government authority in a third d) Probability that in the remaining cases the requested data will be 1% country, based on Art 48 GDPR. Google has explained in reply to this DTIA that it has not provided any personal data from Dutch public provided in one way or another (e.g., with consent or through legal sector customers to law enforcement authorities in the assessment period, also not on a voluntary basis. or administrative assistance) Enforcing lawful access via Google to access Diagnostic Data of one of its public sector customers (where it is a processor) is much more e) Probability that in the remaining cases the authority will consider 50% difficult than in the case of data of private individuals (where it is a controller). It also takes time. Therefore, we believe that the the data it is seeking to be so important that it will look for another authorities will want to undergo such trouble only in particularly important cases, thus significantly reducing the number of relevant way to obtain it 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 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 Based on E37*C21 Step 4a: Probability that a foreign authority will successfully enforce the claim through the provider Unknown for Australia, Brasil, Chile, Hong Kong, India, Singapore and Taiwan, EU Adequacy Decision for registered participants in the EU-US Data Privacy Framework Legal Basis considered for the following assessment: Probability per case Prerequisite for success Google is a well-known cloud services provider with a substantial amount of Workspace for public sector customers in the EU a) Probability that the authority is aware of the provider and its subcontractors (prerequisite no. 1) Customers can intentionally, with consent, allow Google support employees in 12 third countries to access Diagnostic Data in plain text 0,00% b) Probability that an employee of the provider or its subcontractors 0% as part of a support request. It is assumed that Dutch public sector Workspace customers will not consent to such a transfer. However, will gain access to the data in plain text in a support-case ... the Support Data can also be accessed without such consent by subprocessors in Australia, Brasil, Chile, Hong Kong, India, Singapore and (prerequisite no. 2) Taiwan, as part of technical service maintenance and support, but they need to be authorised to access specific data [see below]. Government organisations 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. Google employees can incidentally be tasked to look at problems from Dutch government customers with Meet, but they cannot 'search' .. and is able to search for, find and copy the data requested by the 1% for any customers' personal data, including Diagnostic Data. Google explains: "Access is entirely dependent on the specific activity they authority (prerequisite no. 3) need to perform and only occurs where absolutely necessary to e.g. address the specific technical issue they are investigating." Google 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." As analysed above, CSE cannot be applied to Diagnostic Data. Though Google has not provided any personal data from Dutch public c) Probability that despite the technical countermeasures taken, 10% sector customers to law enforcement in the past 2 years, Google is prohibited from publishing details about disclosure to security employees of the provider, of its subcontractors or of the parent company technically have access to data in plain text (also) outside In reply to this DTIA Google has explained it has not built in any backdoors. "Google has not provided any government with direct access a support situation (e.g., using admin privileges) or are able to gain 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." such access, e.g., by covertly installing a backdoor or "hacking" into Google has clarified that this statement also applies to indirect access through for example, distribution of a new version or temporary the system (irrespective of whether they are allowed to do so) ... lifting of transit encryption. "Google will not disable security features or alter Meet systems to allow third parties to gain access to (prerequisite no. 2) 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. It is not certain that Google would succeed in gaining access and be able to search for the Diagnostic Data specifically requested by an .. and are then able to search for, find and copy the data requested 50% by the authority (prerequisite no. 3) Google explains in its information about subprocessors that its subsidiaries in 7 third countries may have access to the Diagnostic Data d) Probability that the provider, the subcontractor or its parent 100% for the purposes of data centre operations, and for software and systems engineering, maintenance and troubleshooting. See: company, respectively, is located within the jurisdiction of the https://workspace.google.com/terms/subprocessors.html authority (prerequisite no. 4) Probability that despite the technically limited access and the 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 technical and organizational countermeasures in place, the probability that government authorities in the third countries can order Google to provide access to the Diagnostic Data is set to 100%. 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) Privacy Company has studied the confidential SOC-2 and C5:2020 audit reports, but these reports only assess Google's compliance with Probability that if data were to be handed over to the foreign 25% these standards for Content Data, not for the Diagnostic Data Google includes in the term Service Data. The probability is not zero, authority, this would lead to the criminal liability of employees of because Google has a Code of Conduct, which mentions the existence of anti-bribery laws, with the following sentence: "Like all the provider or its subcontractors, the prosecution of which would 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." be possible and realistic, and as a consequence, the data does not 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 have to be produced or is not produced (prerequisite no. 6) third countries is unknown. Google has explained in the past 2 years it has not disclosed any Diagnostic Data belonging belonging to public sector institutions located Probability that the government organisation does not succeed in 100% in the Netherlands in response to requests from law enforcement agencies (such as requests made under warrant or subpoena) based in removing the relevant data in time or otherwise withdrawing it Australia; Brazil; Chile; Hong Kong; India; Singapore; Taiwan; or the United States (US). However, Google does not disclose statistics from the provider's access (prerequisite no. 7) 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. 3,75% Residual risk of successful lawful access by a foreign authority through the provider (given the countermeasures): 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 Google applies encryption in transit for inter-region data traffic and global routing (ALTS and TLS, plus the MTA-STS standard for mail), a) Probability that the data at issue is transmitted to the provider or its 0% and AED for data stored at rest. Google also writes it never gives any government "backdoor" access." In reply to questions about access subcontractors in a manner that permits the telecommunications to encryption keys as part of 'backdoors', Google has further clarified: "Google will not disable security features or alter Meet systems to providers in the country to view it in plain text as part of an allow third parties to gain access to Customer Personal Data that would otherwise be unavailable to a third party in clear text." upstream monitoring of Internet backbones See the explanation in the row above. b) Probability that the data transmitted will include content picked by 0% selectors (i.e., intelligence search terms such as specific recipients or senders of electronic communications) As Google applies the encryption, Google and its subsidiaries are technically capable of lifting that encryption, and can do so in practice Probability that the provider or a subcontractor in the country is 10% for service maintenance, troubleshooting and technical support. Because the names of participants and names of Meets cannot be technically able to on an ongoing basis search the data in plain text encrypted with CSE, the probability that Google performs such a search cannot be excluded. 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 d) Probability that the provider or a subcontractor in the countries 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 above may be legally required to perform such as search (also) with measures (as described by the European Court of Justice and in the recommendations from the EDPB) in place. the company's data 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). It is plausible that Diagnostic Data from a Dutch public sector organisation are interesting for security services in the 7 third countries e) Probability that the data is regarded as content that is the subject of 100% where they may be accessed. Since customers cannot encrypt Diagnostic Data with their own key, and Diagnostic Data reveal who intelligence searches in the country as per the above laws 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 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% 3,75% Probability of successful lawful access by the foreign authorities concerned in these cases despite the countermeasures Probability of additional successful lawful access by a foreign intelligence service where there is no guarantee of legal recourse (despite 0,10% Overall probability of a successful lawful access to data in plain text via the cloud provider in the observation period: Description in words (based on Hillson*): The number of years it takes for a lawful access to occur at least once with a **90 percent** probability: The number of years it takes for a lawful access to occur at least once with a **50 percent** probability: ... 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 a) Estimated probability of occurrence of successful lawful access risk: 3,81% Very Low 3= regular personal data in the clear High This assessment assumes Dutch public sector organisations will follow the recommendation to use pseudonyms for sspecific employees 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 b) Estimated impact of risk personal data is still high, the risk is assessed as low in view of the very low probability that the risk materialises. **Step 7: Define the safeguards in place** Rationale Would it be feasible, from a practical, technical and economical Google does not make a Data Region choice available for Diagnostic Data as part of the Service Data. Google has not disclosed any plans Describe why you still do not 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 a) point of view, for the data exporter to transfer the personal data in Yes pursue this option the 7 third countries. question to a location in a whitelisted country instead? Once a public sector organisation uses Google Meet, the transfer of Diagnostic Data is structural, not incidental. Is the personal data transferred under one of the exemptions b) pursuant to applicable data protection law (e.g., Art. 49 GDPR in case No of the GDPR)? Is the personal data at issue transmitted to the target jurisdiction in Ensure that data remains 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 clear text (i.e. there is no appropriate encryption in-transit)? Diagnostic Data. 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. 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 Foreign lawful access is at least data is either not appropriately encrypted or access to the keys to technically possible decrypt is possible)? The Dutch public sector Enterprise customers can rely on appropriate transfer mechanisms under Chapter V GDPR. Is the personal data at issue protected by a transfer mechanism approved by the applicable data protection law (e.g., the EU Ensure that the mechanism Standard Contractual Clauses in case of the GDPR, approved BCR, or remains in place and is complied 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

Based on the answers given above, the transfer is:

Final Step: Conclusion

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

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

This Transfer Impact Assessment has been made by:

SLM Microsoft, Google Cloud and Amazon Web Services Rijk / PRIVACY COMPANY

Place, Date:
Signed:

Reassess at the latest by: X+2

(or if there are any changes in circumstances)

DTIA continues to distinguish between 6 categories of personal data. This distinction also conferencing) make this DTIA more comparable with other public DTIAs on videoconferencing services. Step 1: Describe the intended transfer COMMENTS GOOGLE Dutch government organisation [X] a) Data exporter (or the sender in case of a relevant onward transfer): [Confidential] for the Dutch public sector. b) Country of data exporter: Google LLC in the USA. The Dutch public sector customers rely on appropriate transfer mechanisms under Chapter V GDPR. c) Data importer (or the recipient in case of a relevant onward transfer): The contracting entity for Dutch public sector 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 d) Country of data importer: 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 e) Context and purpose of the transfer: to take extra measures to protect the personal data. Google Workspace administrators and employee users of Dutch public sector organisations + external participants in Meet conferences (as guest users, or with a Google account). f) Categories of data subjects concerned: 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 g) Categories of personal data transferred: special categories of data. Security logs may be used for criminal investigation, reports and flags may include both sensitive and special categories of data, as well as data about (alleged) criminal offenses. h) Sensitive and special categories of personal data: 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 i) Technical implementation of the transfer: the EDPB and future new CSAM legislation in the EU. No additional technical and organisational measures are required for the transfer to the USA since the adequacy decision from the European Commission from 10 July 2023. The Dutch public 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. j) Technical and organizational measures in place: USA k) Relevant onward transfer(s) of personal data (if any): l) Countries of recipients of relevant onward transfer(s): Step 2: Define the DTIA parameters Rationale a) Starting date of the transfer: [assessment made on 22 October 2024] b) Assessment period in years: 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 USC § 1881(b)(4): Google explains in its "Government Requests for Cloud Customer Data" whitepaper that it commits to object to, or limit or modify, any f) Does importer/processor commit to legally resist every request for No legal process that it reasonably determines to be overbroad, disproportionate, incompatible with applicable law, or otherwise unlawful. access: See Step 2 on page 7. However, this guide does not cover the Service Data. The confidential agreement with the Dutch government includes 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 government does not agree that Google is entitled to such voluntary disclosures. Google has assured the Dutch public sector that it has not disclosed any personal data from Dutch public sector customers in the past 2 years for this purpose. For the transfer to the USA, the updated relevant US laws are 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 g) Relevant local laws taken into consideration: have to be complemented by supplementary measures. The assessment has already been made by the European Commission. analysed by the European Commission in the Data Privacy Framework decision from 10 June 2023. Step 7: Define the safeguards in place Rationale Would it be feasible, from a practical, technical and economical point of Like other hyperscalers, Google operates centralised security services and one Trust and Safety Team in the USA. Though technically Describe why you still do not pursue a) view, for the data exporter to transfer the personal data in question to a Yes possible, Google has no intention to create specific EU security and trust & safety teams. location in a whitelisted country instead? Once a public sector organisation uses Google Meet the transfer is structural, not incidental. 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)? Is the personal data at issue transmitted to the target jurisdiction in clear No, Google by default applies encryption both in-transit and to stored data, but with its own keys. Ensure that data remains encrypted text (i.e. there is no appropriate encryption in-transit)? Yes, authorised Google employees in the USA can technically access the security logs and data for the trust & safety team. Is the personal data at issue accessible in the target jurisdiction in clear Foreign lawful access is at least technically possible d) text by the data importer/recipient or a third party (i.e. the data is either Yes not appropriately encrypted or access to the keys to decrypt is possible)? Is the personal data at issue protected by a transfer mechanism approved The Dutch public sector Enterprise customers can rely on appropriate transfer mechanisms under Chapter V GDPR. 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
Yes Ensure that the mechanism remains in place and is complied with 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)?

Reassess at the latest by: X+2

(or if there are any changes in circumstances)

This DTIA was made by Privacy Company, and SLM Microsoft, Google and Amazon Web Services Rijk, using and adapting the template provided by David Rosenthal, provided under CC license

Data Transfer Impact Assessment (DTIA) on the

transfer to third countries of Content Data

processed by Google Meet (audio/video

Based on the answers given above, the transfer is:

This Transfer Impact Assessment has been made by:

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

SLM Microsoft, Google Cloud and Amazon Web Services Rijk / PRIVACY COMPANY

Final Step: Conclusion

Permitted

Place, Date:

By: Government organisation [X]

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,

differences in both the impact and the probability of unauthorised access to these data, this

Account Data, Diagnostic Data, Security Data and Website Data. Because there are

Admin Console. Google considers Website Data a subsection of Service Data. This DTIA Data Transfer Impact Assessment (DTIA) on the distinguishes between 5 categories of Service Data: data about support tickets, Account transfer to third countries of Content Data processed This DTIA was made by Privacy Company, and SLM Microsoft, Google and Amazon Web Services Rijk, using and adapting the template provided by David Rosenthal, provided under CC license 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 by Google Meet (audio/video conferencing) 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** Dutch government organisation [X] a) Data exporter (or the sender in case of a relevant onward transfer): [Confidential] for the Dutch public sector. Technically, Google maintains servers around the world and its support and service engineers b) Country of data exporter: in the 7 third countries can access data anywhere, if necessary and authorised. Google LLC in the USA. The Dutch public sector customers rely on appropriate transfer mechanisms under Chapter V GDPR. c) Data importer (or the recipient in case of a relevant onward transfer): USA, with onward transfers to third countries for recorded data. The contracting entity for Dutch public sector 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 d) Country of data importer: Limited is a wholly owned subsidiary of Google LLC, which in turn is a wholly owned subsidiary of Alphabet Inc. 2 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 Google has not answered the question if Website Data (including IP addresses) from guest audio. The video conference service also offers related features such as text chatting and file sharing among participants, (Al generated) live captions of speech, and (Al) translations of live captions. users in meetings organised by public sector customers are offered the same processing 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 guarantees. This DTIA assumes there is no such protection umbrella. 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 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 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 public sector 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 e) Context and purpose of the transfer: 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 issue, 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 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 institutions located in the Netherlands in the past two years." Google Workspace administrators and employee users of Dutch public sector organisations + external participants in Meet conferences (as guest users, or with a Google account). f) Categories of data subjects concerned: 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 g) Categories of personal data transferred: identity should remain confidential. none h) Sensitive and special categories of personal data: 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. i) Technical implementation of the transfer: This means the Website Data may be transferred to the 7 third countries as well as the USA where Google processes Service Data. 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. j) Technical and organizational measures in place: Organisational measures: Same as Content and Account Data Website Data from Meet may be transferred to 7 third countries for data center operations, software and systems engineering, maintenance and troubleshooting. k) Relevant onward transfer(s) of personal data (if any): I) 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 22 October 2024] b) Assessment period in years: c) Ending date of the assessment based on the above: d) Target jurisdiction for which the DTIA is made: This includes access to Website Data for service maintenance and for technical support by engineers in these 7 third countries. It is Australia, Brazil, Chile, Hong Kong, India, Singapore and Taiwan + 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 USC § 1881(b)(4): Google explains in its "Government Requests for Cloud Customer Data" whitepaper that it commits to object to, or limit or modify, any f) Does importer/processor commit to legally resist every request for No 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 agreement with the Dutch government includes 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 government does not agree that Google is entitled to such voluntary disclosures. Google has assured the Dutch public sector that it has not disclosed any personal data from Dutch public sector customers in the past 2 years for this purpose. g) Relevant local laws taken into consideration: This DTIA cannot provide a detailed legal analysis of the applicable surveillance laws in the 7 third countries. Absent such an analysis, it Google has not shared its legal analysis of applicable laws and their has to be assumed that some or all authorities in the third countries are permitted to obtain data from Google. compliance with the fundamental right guarantees offered to data subjects 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 in Australia, Brazil, Chile, Hong Kong, India, Singapore and Taiwan. 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 Cases remaining per case In reply to this DTIA Google has stated it has not disclosed any Website Data (as part of Service Data) from Dutch public sector customers a) Number of cases under the laws listed in Step 2g per year in which an 100% to law enforcement in the past two years: "We can confirm that, in the past two years (which we understand to be your 'assessment authority in the third countries is estimated to attempt to obtain relevant period'), we have not disclosed any Customer Data or Service Data belonging to public sector institutions located in the Netherlands in data through <u>legal action</u> during the period under consideration. 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. 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 b) Share of such cases in which the request occurs in connection with a case 100% 1,00 are permitted to obtain data from Google. For example, as Hong Kong is part of China, governments across the EU have expressed that due to its nature in principle permits the authority to obtain the data concerns about access by Chinese authorities to personal data from EU citizens. As quoted above, though Google has not disclosed any also from a provider Dutch public sector 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. CSE is not available for Website Data. Therefore, the probability that Google is not able to produce these data in clear text, is zero. c) Probability that in the remaining such cases it will be possible for the 0% company to successfully cause the authority (by legal means or otherwise) to give up its request for the data in plain text Absent an MLAT with the third country, EU organisations cannot consent to disclose Website Data to a government authority in a third d) Probability that in the remaining cases the requested data will be country, based on Art 48 GDPR. Google has explained in reply to this DTIA that it has not provided any personal data from Dutch public provided in one way or another (e.g., with consent or through legal or sector customers to law enforcement authorities in the assessment period, also not on a voluntary basis. administrative assistance) e) Probability that in the remaining cases the authority will consider the data 50% Enforcing lawful access via Google to access Website Data from end users and admins of one of its public sector 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 it is seeking to be so important that it will look for another way to obtain 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 Based on E35, which is a calculation of C35*D34. D34 is calculated as (1-C34)*D33 0,90 Number of cases in the period under consideration Based on E37*C21 Step 4a: Probability that a foreign authority will successfully enforce the claim through the provider 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 Legal Basis considered for the following assessment: Prerequisite for success Probability per case Google is a well-known cloud services provider with a substantial amount of public sector Workspace customers in the EU a) Probability that the authority is aware of the provider and its subcontractors (prerequisite no. 1) 0,00% The Website Data can be accessed without consent from customers by subprocessors in Australia, Brazil, Chile, Hong Kong, India, b) Probability that an employee of the provider or its subcontractors will gain 0% Singapore and Taiwan for data centre operation and technical support purposes. Google has explained that customers can view the access to the data in plain text in a support-case .. (prerequisite no. 2) 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 Google employees can incidentally be tasked to look at problems from Dutch customers with Meet, but they cannot 'search' for any .. and is able to search for, find and copy the data requested by the customers' personal data, including Diagnostic Data. Google explains: "Access is entirely dependent on the specific activity they need to authority (prerequisite no. 3) 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." As analysed above, CSE cannot be applied to Website Data. Though Google has not provided any personal data from Dutch public sector c) Probability that despite the technical countermeasures taken, employees 10% 5,00% customers to law enforcement in the past 2 years, Google is prohibited from publishing details about disclosure to security services. of the provider, of its subcontractors or of the parent company technically In reply to this DTIA Google has explained it has not built in any backdoors. "Google has not provided any government with direct access have access to data in plain text (also) outside a support situation (e.g., to any information stored in our data centers, including data stored or processed by the Meet application." Google has also stated: using admin privileges) or are able to gain such access, e.g., by covertly "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 installing a backdoor or "hacking" into the system (irrespective of whether transit encryption. "Google will not disable security features or alter Meet systems to allow third parties to gain access to Customer they are allowed to do so) ... (prerequisite no. 2) 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. It is not certain that Google would succeed in gaining access and be able to search for the Website Data specifically requested by an .. and are then able to search for, find and copy the data requested by the 50% authority (prerequisite no. 3) Google explains in its information about subprocessors that its subsidiaries in 7 third countries may have access to the Diagnostic Data for d) Probability that the provider, the subcontractor or its parent company, 100% 100% data centre operations and for software and systems engineering, maintenance and troubleshooting. See: respectively, is located within the jurisdiction of the authority (prerequisite no. https://workspace.google.com/terms/subprocessors.html Speculative estimate. Though Google by default applies encryption to data-at-rest, including Website Data, Google has access to these e) Probability that despite the technically limited access and the technical 100% keys, can use these keys to decrypt if necessary for troubleshooting, and can hence also be ordered to decrypt the data. Therefore the and organizational countermeasures in place, the authority is permitted to probability that government authorities in the third countries can order Google to provide access to the Website Data is set to 100%. 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) Privacy Company has studied the confidential SOC-2 and C5:2020 audit reports, but these reports only assess Google's compliance with Probability that if data were to be handed over to the foreign authority, 25% 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 this would lead to the criminal liability of employees of the provider or its Code of Conduct, which mentions the existence of anti-bribery laws, with the following sentence: "Like all businesses, Google is subject to subcontractors, the prosecution of which would be possible and realistic, lots of laws, both U.S. and non-U.S., that prohibit bribery in virtually every kind of commercial setting." URL: and as a consequence, the data does not have to be produced or is not 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 produced (prerequisite no. 6) third countries is unknown. Google has explained in the past 2 years it has not disclosed any Website Data belonging to public sector institutions located in the Probability that the government organisation does not succeed in 100% Netherlands in response to requests from law enforcement agencies (such as requests made under warrant or subpoena) based in removing the relevant data in time or otherwise withdrawing it from the Australia; Brazil; Chile; Hong Kong; India; Singapore; Taiwan; or the United States (US). However, Google does not disclose statistics about provider's access (prerequisite no. 7) 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 Unknown for Australia, Brazil, Chile, Hong Kong, India, Singapore and Taiwan, EU Adequacy Decision for the USA including FISA Legal Basis considered for the following assessment: Probability in the period Google applies encryption in transit for inter-region data traffic and global routing (ALTS and TLS, plus the MTA-STS standard for mail), a) Probability that the data at issue is transmitted to the provider or its 0,00% and AED for data stored at rest. Google also writes it never gives any government "backdoor" access." In reply to questions about access to subcontractors in a manner that permits the telecommunications encryption keys as part of 'backdoors', Google has further clarified: "Google will not disable security features or alter Meet systems to allow providers in the country to view it in plain text as part of an upstream third parties to gain access to Customer Personal Data that would otherwise be unavailable to a third party in clear text." monitoring of Internet backbones b) Probability that the data transmitted will include content picked by 0% selectors (i.e., intelligence search terms such as specific recipients or senders of electronic communications) c) Probability that the provider or a subcontractor in the country is As Google applies the encryption, Google and its subsidiaries are technically capable of lifting that encryption, and can do so in practice for 0,05% service maintenance, troubleshooting and technical support. The probability that Google performs such a search for an IP address or the technically able to on an ongoing basis search the data in plain text for unique cookie identifier from the NID-cookie cannot be excluded. 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 Speculative estimate. This refers to Upstream Data Collection. According to the Adequacy Decision from the European Commission, Probability that the provider or a subcontractor in the countries above may 1% personal data may be transferred to the USA without having to put additional measures in place, but no such analysis is available for the be legally required to perform such as search (also) with the company's 7 third countries. It is plausible that some Website Data from a Dutch public sector 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 50% It is plausible that Website Data from a Dutch public sector 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 intelligence searches in the country as per the above laws 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** 90,00% Probability that the question of lawful access via the cloud provider will arise at all (1 case in the period = 100%) 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 0,05% 3,43% Overall probability of a successful lawful access to data in plain text via the cloud provider in the observation period: 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: The number of years it takes for a lawful access to occur at least once with a **50 percent** probability: ... 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 a) Estimated probability of occurrence of successful lawful access risk: 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 these personal data is low. In view of the very low probability that the risk of unauthorised access materialise, the risk is assessed as low. b) Estimated impact of risk Though there are no high risks anymore for the transfer to the USA, such quarantees are not available for transfer to Google's data centres in Australia; Brazil; Chile; Hong Kong; India; Singapore and Taiwan. **Step 7: Define the safeguards in place** Rationale Would it be feasible, from a practical, technical and economical point of 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 Describe why you still do not pursue limit access to Service Data to EU-based engineers only. This means the Website Data can be processed by support engineers in the USA, a) view, for the data exporter to transfer the personal data in question to a Yes this option and in the 7 third countries. location in a whitelisted country instead? Once a public sector organisation uses Google Meet, the transfer of Website Data is structural, not incidental. 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)? Is the personal data at issue transmitted to the target jurisdiction in clear 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 Ensure that data remains encrypted text (i.e. there is no appropriate encryption in-transit)? 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. Is the personal data at issue accessible in the target jurisdiction in clear Foreign lawful access is at least d) text by the data importer/recipient or a third party (i.e. the data is either Yes not appropriately encrypted or access to the keys to decrypt is possible)? The Dutch public sector Enterprise customers can rely on appropriate transfer mechanisms under Chapter V GDPR. 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 place and is complied with 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)?

Based on the answers given above, the transfer is:

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

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 Microsoft, Google Cloud and Amazon Web Services Rijk / PRIVACY COMPANY

Place, Date:

Signed:

By: Government organisation [X]