

<p>Would it be possible, from a practical, technical and economic point of view, for the data exporter to transfer the personal data to a question to a location in a whitelisted country instead?</p>	<p>Yes</p>	<p>Excludes why you did not answer this question</p>	<p>Google allows its Developer Customer customers to which data in the EU to use the Google Data Flow... (text continues)</p>
<p>Is the personal data transferred under one of the exemptions pursuant to applicable data protection law (e.g., Art. 6(1)(f) GDPR) in case No. of the GDPR?</p>	<p>No</p>	<p>Excludes why you did not answer this question</p>	<p>Even though the possibility of access to the requested information in the data stored in the EU is very small, user or public sector information and Google Maps the transfer is not possible.</p>
<p>Is the personal data at issue transmitted to the target jurisdiction in clear text (i.e., there is no appropriate encryption in-transit)?</p>	<p>No</p>	<p>Excludes why you did not answer this question</p>	<p>No, Google is not able to offer encryption both on transit and to stored data, but with our best efforts, customers can display data with their data to be clear. (text continues)</p>
<p>Is the personal data at issue accessible in the target jurisdiction in clear text to 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 available)?</p>	<p>Yes</p>	<p>Excludes why you did not answer this question</p>	<p>Google has no access to the data stored in the EU, which is not possible and necessary. Google has not shared any data to the extent of its data engineering and the data is not accessible to any of our employees and partners. (text continues)</p>
<p>Is the personal data at issue protected by a transfer mechanism approved by the applicable data protection law (e.g., the EU Standard Contract 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 GDPR), and can you expect compliance with it, under the law of the target jurisdiction and judicial enforcement?</p>	<p>Yes</p>	<p>Excludes why you did not answer this question</p>	<p>The Dutch Adult User Privacy Statement contains an appropriate transfer mechanism under Chapter 9 GDPR.</p>

Based on the answers given above, the transfer of sensitive and special categories of data without CSE is:

Not Permitted

Final Step: Conclusion

In view of the above and the applicable data protection laws, the transfer of sensitive and special categories of data without CSE is:

not permitted

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

permitted

This transfer impact assessment has been made by:

IBM Research, Google Cloud and Amazon Web Services / ANNOVA COMPANY

Place, Date:
Signed:
By: Government organisation [X]



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 third-country jurisdiction?	Yes	Does not apply as it is not a public sector institution	Google does not make a Data Region choice available for Account Data, nor as part of the Content Data, and not as part of the Source Data. Google has not disclosed any plans to limit the access to its board members only. This means the Account Data can be processed by support engineers in the USA and in EU 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 both engineers in third countries to the Account Data is very small, since a public sector institution can Google Maps the transfer is not considered as restricted.
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	Personal data is not encrypted	As Google by default applies encryption both in transit and in stored data, but with its own keys, it is not possible to apply CCF or the Account Data.
d) Is the personal data at issue accessible in the target jurisdiction in clear text by the data importer/recipient or a third party (i.e. the data is either not appropriately encrypted or access to the keys to decrypt is possible)?	Yes	Foreign law enforcement has access to the data	Yes, Google and its subsidiaries in 3rd 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	Also valid for the public sector in the target jurisdiction	The third public sector institution customer uses only an appropriate transfer mechanism under Chapter V GDPR.

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

Final Step: Conclusion
In view of the above and the applicable data protection laws, the transfer is: permitted Revised at the latest by: v2

This Transfer Impact Assessment has been made by: Date: _____
J.M. Microsoft, Google Cloud and Amazon and Services Agp / Agency customer Signed: _____
By: Government organisation [1]

Final Step: Conclusion

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

personal data

Reasons at the label: 142

This Transfer Impact Assessment has been made by:
IAM Microsoft, Google Cloud and Amazon AWS Service RFP / PANTRY CDMAKRY

Place, Date:
Signed:
By: Government Organisation [X]

(or if there are any changes in circumstances)

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

is

This Transfer Impact Assessment has been made by:
GAC/Ministry of Social Development Services (MSS) / [PRIVACY OFFICER](#)

Place, Date:
Signed:

By: Government Organisation (X)

Reasons of the label: X(1)

(or if there are no changes to (X)(1)(a)(i))

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



This DTIA was made by Privacy Company, and SAM Microsoft, Google and Amazon Web Services, LLC, using and adapting the template provided by David Hoarehead, provided under CC license

This tab describes the transfers of Security logfiles, and reports processed by Google's Trust & Safety team to the USA. Google considers these security data a subsection of Service Data. This DTIA distinguishes between 5 categories of Service Data: data about support tickets, Account Data, Diagnostic Data, Security Data and Website Data. Because there are differences in both the impact and the probability of unauthorised access to these data, this DTIA continues to distinguish between 6 categories of personal data. This distinction also makes 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.	
b) Country of data exporter:		
c) Data importer (or the recipient in case of a relevant onward transfer):	Google LLC in the USA. The Dutch public sector customers rely on appropriate transfer mechanisms under Chapter V GDPR.	
d) Country of data importer:	USA The contracting entity for Dutch public sector customers of Google Workspace is Google Cloud EMEA Limited (see https://cloud.google.com/terms/google-emty), a Google entity based in Dublin, Ireland. Google Cloud EMEA Limited is a wholly owned subsidiary of Google LLC, which in turn is a wholly owned subsidiary of Alphabet Inc.®	
e) Context and purpose of the transfer:	This assessment is based on the exclusive transfer of Security logs and notifications to the Trust & Safety Team in the USA. Based on the adequacy decision for the data protection regime in the USA, organisations do not have to take extra measures to protect the personal data.	
f) Categories of data subjects concerned:	Google Workspace administrators and employee users of Dutch public sector organisations + external participants in Meet conferences (as guest users, or with a Google account).	
g) Categories of personal data transferred:	Security logs may reveal information about malicious attackers, such as their IP addresses and types of devices used. Reports to the Trust & Safety Team, as well as flags of suspected CSAM may include regular, sensitive and special categories of data.	
h) Sensitive and special categories of personal data:	Security logs may be used for criminal investigation, reports and flags may include both sensitive and special categories of data, as well as data about (alleged) criminal offenses.	
i) Technical implementation of the transfer:	Security logs are kept by Google LLC in the USA. The Trust & Safety team works in the USA. Google has confirmed it does not use AI to scan for unknown CSAM material, and has committed to comply with the guidance from the EDPB and future new CSAM legislation in the EU.	
j) Technical and organisational measures in place:	No additional technical and organisational measures are required for the transfer to the USA since the adequacy decision from the European Commission 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.	
k) Relevant onward transfer(s) of personal data (if any):	USA	
l) Countries of recipients of relevant onward transfer(s):	USA	

Step 2: Define the DTIA parameters

		Rationale
a) Starting date of the transfer:	[assessment made on 22 October 2024]	
b) Assessment period in years:	2	
c) Ending date of the assessment based on the above:	X+2	
d) Target jurisdiction for which the DTIA is made:	United States (exclusively)	
e) Is importer an Electronic Communications Service Provider as defined in UIC's (SAR) (16):	Yes	
f) Does importer/processor commit to legally resist every request for access:	No	Google explains in its "Government Requests for Cloud Customer Data" whitepaper that it commits to resist to, or limit or modify, any such requests that it reasonably determines to be overbroad, disproportionate, incompatible with applicable law, or otherwise unlawful. See Step 2 on page 7. However, this public does not cover the Service Data. The confidentiality agreement with the Dutch government includes detailed commitments with regard to disclosure. Google has also explained in reply to this DTIA that it exclusively engages voluntarily in a request from a Third Country authority by disclosing only limited USA personal data in emergency situations where it has a good faith belief that disclosure of USA personal data to 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:	For the transfer to the USA, the updated relevant US laws are analysed by the European Commission in the Data Privacy Framework decision from 10 June 2023.	Since the adequacy decision for the USA from the European Commission on 10 July 2023, transfers to the USA based on the DPF do not have to be complemented by supplementary measures. The assessment has already been made by the European Commission.

Step 3: Define the safeguards in place

		Rationale
a) Would it be feasible, from a practical, technical and economic point of view, for the data exporter to transfer the personal data in question to a location in a whitelisted country instead?	Yes	Unlike other Applications, Google operates centralised security services and one Trust and Safety team in the USA. Though technically possible, Google has no intention to create specific EU security and trust & safety teams.
b) Is the personal data transferred under one of the exemptions pursuant to applicable data protection law (e.g., Art. 49 GDPR in case of the GDPR)?	No	Other public sector organisations use Google Meet the transfer is a situation, 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	No, Google by default applies encryption both in-transit and to stored data, but with its own keys.
d) Is the personal data at issue accessible in the target jurisdiction in clear text by the data importer/recipient or a third party (i.e. the data is either not appropriately encrypted or access to the keys to decrypt is possible)?	Yes	Yes, authorised Google employees in the USA can technically access the security logs and data for the trust & safety team.
e) Is the personal data at issue protected by a transfer mechanism approved by the applicable data protection law (e.g., the EU Standard Contractual Clauses in case of the GDPR, approved BCR, or in the case of an onward transfer - a back-to-back contract in line with the EU SCCs), and can you expect compliance with it, insofar as permitted by the target jurisdiction, and judicial enforcement (where applicable)?	Yes	The Dutch public sector Enterprise customers can rely on appropriate transfer mechanisms under Chapter V GDPR.

Based on the answers given above, the transfer is:

Permitted

Final Step: Conclusion

In view of the above and the applicable data protection laws, the transfer is:	permitted	Reassess at the latest by: X+2
		(or if there are any changes in circumstances)

This Transfer Impact Assessment has been made by:
SAM Microsoft, Google Cloud and Amazon Web Services EMEA / PRIVACY COMPANY

Place, Date,
Signed:

By: Government organisation [X]

Final Step: Conclusion

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

permitted

Reasons of the latest by: X12

(or if there are any changes in circumstances)

This Transfer Impact Assessment has been made by:
S&B Group Ltd, Group Chief Information Officer / AGENCY COMPANY

Place, Date:
Signed:

By: Government organisation [X]