



|   |     |
|---|-----|
| Google shares its Developer Customer's location information in the EU to meet the Content Data Flow Model. See Google Data Transfer Customer Agreement for more details. <a href="https://support.google.com/ads/answer/1048606">https://support.google.com/ads/answer/1048606</a> is Google explains how the content data is shared with third parties to ensure their marketing, including third parties, in the "Other content data model" advertisement reports, including results, frequency, duration, the content of ads, and content Google's "for example" with its publicly accessible reports of the data reported to our Developer Customer and how it is used to report results for report results and/or of the EU, processing in Google along with its in Google's report for the end of 2022. See <a href="https://support.google.com/ads/answer/1048606">https://support.google.com/ads/answer/1048606</a> . |     |
| 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 |
| Describe why you did not answer this question   |     |
| b) Is the personal data transferred under one of the exemptions pursuant to applicable data protection law (e.g., Art. 49 GDPR)? In case No of the GDPR?  | No  |
| 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  |
| Describe the data transfer  |     |
| d) Is the personal data at issue accessible in the target jurisdiction to clear text by the data importer/recipient or a third party (i.e. the data is either not appropriately encrypted or access to the key to decrypt is possible)?   | Yes |
| Describe how/when and how technically possible  |     |
| e) 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 ECR, 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, under permitted by the target jurisdiction, and judicial enforcement  | Yes |
| Describe the mechanism and when/when is compliant with  |     |
| The Dutch public sector (public sector) customers can rely on appropriate transfer mechanisms under Chapter V GDPR.   |     |
| Based on the answers given above, the transfer of sensitive and special categories of data without CSE is:  |     |
| Not Permitted   |     |

Final Step: Conclusion

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

not permitted

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

permitted

This Transfer Impact Assessment has been made by: [IAM Germany, Google Cloud and Amazon Web Services / Privacy Compliance](#)

Page: 2/2

By: Government organisation [X]



This table describes the transfer of **Account Data**. For Google, Account Data are part of **Service Data**. See: [https://cloud.google.com/terms/cloud-privacy-notice#Then\\_Google\\_explains:Service\\_data\\_consists\\_of\\_Account\\_information](https://cloud.google.com/terms/cloud-privacy-notice#Then_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 (usernames, 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 Contact Data, but not of Account Data. Because the transfer of Account Data has a significant impact and the probability of unauthorized 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.

Google has not answered the question if Google Account Data from guest users in meetings organised by public sector customers are offered the same processing guarantees. This DTIA assumes there is no such protection umbrella.

**Note Privacy Company:** Google does not ask for specific consent for the transfer of Account Data (as part of Google's category of Service Data) to employees in the first list of 12 third countries: the support employees only ask for consent to access to Content or Service Data of the customer without informing the customer in what country they operate. That is why this DTIA assumes that government organisations will not provide such consent.

---

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

Does the data you export not pose this risk?

No

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

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

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

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

Does the data remain encrypted?

Foreign legal enforcement is not necessary to ensure

Does the transfer mechanism comply with applicable requirements?

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 make this option to EU-based engineers only. This means the Account Data can be processed by support engineers in the USA, and at the 7 third countries.

Even though the probability of access by such engineers in third countries to the Account Data is very small, once a public sector organisation uses Google Meet the transfer is subject to a review.

As Google by default applies encryption both in transit and to stored data, but with its own keys, it is not possible to apply CTR to the Account Data.

Yes, Google and its subsidiaries in 3rd countries are technically access the unencrypted Account Data, although this would be a violation of policy and organisational measures.

The Dutch public sector/Chaparral 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

Revisits at the latest by: x+2

This Transfer Impact Assessment has been made by:  
J.M. Microsoft, Google Cloud and Amazon Web Services AG / PRIVACY COUNCIL

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

per if there are any changes in circumstances



Final Step: Conclusion

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

permitted

Reasons at the latest by: 31-2

(or if there are any changes in circumstances)

This Transfer Impact Assessment has been made by:  
S&M Microsoft, Google Cloud and Amazon Web Services AB / PRIVACY COMPANY

Place, Date:

Signed:

By: Government organisation [X]



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

permitted

This Transfer Impact Assessment has been made by:  
S&P Microsoft Group Cloud and Services team / [Privacy Compliance](#)

Place, Date:  
Signed:

By: Government organisation [X]

Revisors at the latest by: N/A

(or if there are any changes to requirements)

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 Rijk, using and adapting the template provided by David Rowenthal, 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 5 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

|    |   |   |
|----|---|---|
| a) | Data exporter (or the sender in case of a relevant onward transfer):    | Dutch government organisation [X]<br>[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<br>The contracting entity for Dutch public sector customers of Google Workspace is <b>Google Cloud EMEA Limited</b> (see <a href="https://cloud.google.com/terms/google-entity">https://cloud.google.com/terms/google-entity</a> ), 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 GDPR 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

|    |  |   |   |
|----|--|---|---|
| a) | Starting date of the transfer:   | [assessment made on 22 October 2024]  | Rationale   |
| 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 USC § 1861(4)? | Yes   | Google explains in its "Government Requests for Cloud Customer Data" whistleblower that it commits to object to, or limit or modify, any legal pressure that it reasonably believes 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.   |
| f) | Does importer/processor commit to legally resist every request for access:             | No  | 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 occasionally responds - voluntarily - to a request from a Third Country authority by disclosing very limited USA personal data in emergency situations where it has a good faith belief that disclosure of USA 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:  | 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

|    |  |     |  |   |
|----|--|-----|--|---|
| 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                 | Rationale   |
| 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  |  | Like other hypercoders, 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.   |
| 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                               | Once a public sector organisation uses Google Meet the transfer is structural, not incidental.  |
| 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 intel access is at most technically possible             | Yes, Google by default applies encryption both in-transit and to stored data, but with its own keys. Yes, authorized 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 BCRs 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 compliant with | 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<br>(or if there are any changes in circumstances) |
|--|-----------|--|

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

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



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

Google has not answered the question if Website Data (including IP addresses) from guest users in meetings organised by public sector customers are offered the same processing guarantees. This DTIA assumes there is no such protection umbrella.

Final Step: Conclusion

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

permitted

Revises at the latest by: N+2

(or if there are any changes in circumstances)

This Transfer Impact Assessment has been made by  
S&P Account - Single Chat and Email Web Service (EU) / PRIVACY COMWAY

Place, Date:

Signed:

By: Government organisation [X]