From:	ve_curia.dpd (CURIA) <dataprotectionofficer@curia.europa.eu>
To:	European Data Protection Supervisor <EDPS@edps.europa.eu>
CC:	ZERDICK Thomas <thomas.zerdick@edps.europa.eu>
Sent at:	01/09/22 17:16:01
Subject:	Your reference: C 2021-0255 (Cisco ad hoc contractual clauses) - Ares(2022)6074690

Your reference: C 2021-0255 (Cisco ad hoc contractual clauses) - Ares(2022)6074690 (Please use this link only if you are an Ares user – Svp, utilisez ce lien exclusivement si vous êtes un(e) utilisateur d'Ares)

Dear Sir,

Please find enclosed a letter and its annexes with regard to a request for authorisation in accordance with Article 48(3)(a) of Regulation (EU) 2018/1725 of new ad hoc contractual clauses to be concluded between Cisco and the Court of Justice of the European Union.

Best regards,

[redacted]

Rue du Fort N edergrünewa d
L-2925 Luxembourg
cur a.europa.eu
[redacted]

SUPPLEMENTARY AGREEMENT No. 1
TO
"Cisco and Court of Justice of the European Union Enterprise License Agreement (ELA)"

BETWEEN

The European Union, represented by the Court of Justice of the European Union, represented, as regards the signing of this supplementary agreement, by Ms. Raluca Peica, Director-General, Directorate-General of Information, hereinafter referred to as *the "Customer"*,

AND

Cisco International Limited, the registered office of which is located at 9-11 New Square, Bedfont Lakes, Feltham, Middlesex TW14 8HA, United Kingdom, represented by....., acting in his/her capacity as an authorized signatory, hereinafter referred to as *the "Supplier" or "Cisco"*,

who have agreed the following:

ARTICLE 1 - SUBJECT OF THE AMENDMENT

1) The purpose of this supplementary agreement No. 1 (the "Amendment") to the Cisco and Court of Justice of the European Union Enterprise License Agreement (ELA) (the "Agreement") is to address the requirements set by the European Data Protection Supervisor in its decision of 31 August, 2021 authorising temporarily the use of ad hoc contractual clauses between the Court of Justice of the EU and Cisco for transfers of personal data in the Court's use of Cisco Cloud Services and the related ELA Support services.

2) The last paragraph of Article 4 of the Agreement is deleted.

3) Article 7.5 of the Agreement is deleted in its entirety.

4) Article 11.2 of the Agreement, titled "Processing of Personal Data by the Supplier", is deleted in its entirety and replaced by the following clause:

"(a) The subject matter and purpose of the processing of personal data under this Agreement is:

(i) Management of this Agreement and any related contractual or financial documents, for which purpose personal data of the Customer's contacts indicated in Article 8, as well as any other staff of the Customer interacting with the Supplier may be processed;

(ii) Cloud Services - provision of web-based videoconferencing services in different formats - meetings with equal participants, meetings/presentations for a wide audience for events in a panel/audience format, training sessions and any other related formats that might be offered as part of the Cloud Service during the period

of the Agreement. In all cases, participants can be Members, staff, external contractors or invitees of the European Union. Internal participants have accounts based on their personal data (email). External participants supply their information at time of logging in into the system with their desired name, potentially providing personal data, based on a shared link and code provided for a specific session;

(iii) Provision of support for ELA Software and Cloud Services, in line with Article 6, for which purpose personal data (contact information) of Customer's staff or external contractors involved in the operation of Subscription Deliverables may be processed.

Personal data under this Agreement is processed in connection to the points listed above, in the United Kingdom, and on servers located in Frankfurt (Germany) (with backup in Amsterdam, The Netherlands), except as otherwise explicitly stated in Annex 1a and Annex 1b to Exhibit A and the Privacy Data Sheets enclosed in Exhibit D (Attachments 1 and 2) attached herein below (with particular regard to the exclusions identified in section 4 – "Webex Data Residency" – of the Webex Meetings Privacy Data Sheet in Exhibit D).

(b) The rules set out in paragraph (c) below apply to the Processing of Personal Data by the Supplier. The other rules set out in paragraph (d) applies specifically to the transfer of Personal Data to third countries under the Agreement.

(c) The Processing of Personal Data by the Supplier shall meet the requirements of Regulation (EU) No 2018/1725, as applicable to the processor, and be processed solely for the purposes set out by the Controller specified in this Agreement, as well as for the purposes listed in Exhibits A to D attached herein below.

Under no circumstances Supplier shall lease, sell, distribute, or otherwise encumber Personal Data (unless mutually otherwise agreed to by a separate signed, written agreement).

The Supplier, acting as the processor in the meaning of Article 3(12) of Regulation (EU) 2018/1725, shall assist the Customer, acting as the controller in the meaning of Article 3(8) of Regulation (EU) 2018/1725, for the fulfilment of the controller's obligation to respond to requests for exercising rights of person whose Personal Data is processed in relation to this Agreement as laid down in Chapter III (Articles 14-25) of Regulation (EU) No 2018/1725. The Supplier shall inform without undue delay the controller about such requests if received directly. The Supplier shall cooperate, on request, with the European Data Protection Supervisor in the performance of its tasks.

The Supplier may act only on documented written instructions – being these as laid down in this Agreement and its Exhibits (or any mutually agreed amendment to this Agreement), and under the supervision of the controller, in particular with regard to the purposes of the Processing, the categories of data that may be processed, the recipients of the data and the means by which the data subject may exercise its rights.

Instructions, in a broader context, shall also mean technical configuration activities performed by Supplier on the request of Customer as well as technical configuration activities, if any, which the Customer may undertake to perform on the ELA Software and/or the Cloud Services within

the standard feature options available for these. For the avoidance of doubt, this means that any configuration applied by the Customer via technical means is to be considered an instruction, but as well that the Customer may not request additional customization to create additional configuration options on the basis of this Agreement. The Supplier will take into account any requests for additional options only in the context of product evolution via its established channels for customer feedback and feature requests and will accept and/or prioritize such requests at the Supplier's discretion. The Supplier will respect and implement any instructions received via the configuration procedure and will not override or change configuration options once set by the Customer, except in cases of ELA Software and/or Cloud Service upgrades, where, due to product evolution, the configuration options change and need to be (re)set. Any such changes must be documented in appropriate changelogs or similar documents and the Customer must be notified of the changes via Supplier's standard customer notification channels (receiving these through the Control Hub Reporting dashboard and the Customer may subscribe to an alias to receive notifications when such alias becomes available).

The Supplier shall grant personnel access to the data to the extent strictly necessary for the implementation, management and monitoring of the Agreement, namely the provision of the ELA Software, Cloud Service and ELA Maintenance/Support. The Supplier must ensure that personnel authorised to process personal data has committed itself to confidentiality or is under appropriate statutory obligation of confidentiality in accordance with the provisions of Article 18.

The Supplier shall adopt appropriate technical and organisational security measures, giving due regard to the risks inherent in the processing and to the nature, scope, context and purposes of processing, in order to ensure, in particular, as appropriate:

(i) the pseudonymisation and encryption of personal data;
(ii) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
(iii) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
(iv) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing;
(v) measures to protect personal data from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to personal data transmitted, stored or otherwise processed.

The appropriate technical and organisational security measures shall be at least those mentioned in Exhibit C to this Agreement.

The Supplier shall notify relevant Personal Data breaches to the controller without undue delay and at the latest within forty-eight (48) hours after the Supplier becomes aware of the breach. In such cases, the Supplier shall provide the controller with at least the following information:

(i) nature of the Personal Data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
(ii) likely consequences of the breach;

(iii) measures taken or proposed to be taken to address the breach, including, where appropriate, measures to mitigate its possible adverse effects.

The Supplier shall without undue delay inform the data controller if, in its opinion, an instruction infringes Regulation (EU) 2018/1725, Regulation (EU) 2016/679, or other Union or Member State data protection provisions.

The Supplier shall assist, as reasonably practical, the controller for the fulfilment of its obligations pursuant to Article 33 to 41 under Regulation (EU) 2018/1725 to:

(i) ensure compliance with its data protection obligations regarding the security of the processing, and the confidentiality of electronic communications and directories of users;
(ii) notify a personal data breach to the European Data Protection Supervisor;
(iii) communicate a personal data breach without undue delay to the data subject, where applicable;
(iv) carry out data protection impact assessments and prior consultations as necessary.

The Supplier shall maintain a record of all data processing operations carried on behalf of the controller, transfers of personal data, security breaches, responses to requests for exercising rights of people whose personal data is processed and requests for access to personal data by third parties.

The Customer is subject to Protocol 7 of the Treaty on the Functioning of the European Union on the privileges and immunities of the European Union, particularly as regards the inviolability of archives (including the physical location of data and services as set out in this Article) and data security, which includes personal data held on behalf of the Customer in the premises of the Supplier or subcontractor.

Without prejudice to the rules set out in paragraph (d), the Supplier shall notify the Customer without delay of any legally binding request for disclosure of the personal data processed on behalf of the Customer made by any international organisation, any national authority (including an authority from a third country), or any other legal or natural person. Unless required to do otherwise by applicable law, the Supplier may not give such access without the prior written authorisation of the Customer. In case where the Supplier is prohibited from notifying the Customer, the Supplier shall challenge the request by exhausting potentially viable remedies, including interim measures, and shall use reasonable efforts to obtain the right to waive this prohibition in order to communicate as much information as they can and as soon as possible to the Customer. The Supplier shall include in its Transparency Report all requests for personal data (processed on behalf of the Customer) received from third parties.

The duration of processing of personal data by the Supplier will not exceed the period referred to in Exhibit D to this Agreement. Upon expiry of the subscription period for the Subscription Deliverables, the Supplier shall, at the choice of the controller, return, without any undue delay in a commonly agreed format, all personal data processed on behalf of the controller and the copies thereof or shall effectively delete all personal data unless Union or national law requires a longer storage of personal data.

The Supplier certifies with regard to the ELA Cloud Services being free of functions that may affect the Personal Data integrity, confidentiality and availability, that Supplier has not intentionally:

(i) created certain programming functions to be used to access, transmit or send the Personal Data without authorization from the Customer;
(ii) created or changed its operational processes regarding Processing of Personal Data in a manner that facilitates access/change/manipulation to the Personal Data other than authorized under the Agreement and its Exhibits, and
(iii) created or maintained programming functions designed to facilitate access by a public authority to Personal Data.

The Supplier shall not engage other (sub-)processors than those listed in Exhibit B, without notifying Customer and providing Customer an opportunity to object. The Supplier shall inform the controller of any material changes in the processing (that may affect the now-current texts of the Data Privacy Sheet in Exhibit D), as well as any intended changes concerning the addition or replacement of other processors (subject to the prior subscription by the Customer in the Cisco Trust Portal) at least one (1) month in advance or as early as practically possible (if so), thereby giving the controller the opportunity to object to such changes. If Customer objects a new Sub-processor and a common solution is not found, Customer may terminate the Agreement in accordance with Article 19.

If part or all of the processing of personal data is subcontracted to a third party, the Supplier shall pass on the essentially equivalent obligations to those referred to in this Article in writing to those parties, including subcontractors. At the request of the Customer, the Supplier shall provide a document providing evidence of this commitment. The Customer and Supplier shall have the possibility to bilaterally review the provisions of this Agreement on Personal Data transfers to continue improving, as needed and/or appropriate, the level of personal data protection in line with the principles of the Regulation (EU) 2018/1725 and having regard to the European Data Protection Supervisor's recommendations or instructions.

Clause 9 of the *Ad hoc* Contractual Clauses (AhCCs) incorporated in Exhibit A applies if the use of a sub-processor by the Supplier implies the transfer of personal data to a third country, insofar as this transfer is not covered by a decision adopted by the European Commission based on Article 45 of Regulation (EU) 2016/679.

Furthermore, the Supplier certifies that:

(i) it does not access the data of the data exporter by default (i.e., without a support request);
(ii) it will provide remote TAC only in case a Single Point of Contact (SPoC) from the data exporter makes a formal request, in which case it will be provided manually with the minimum amount of anonymized data needed for the resolution of the problem, and
(iii) apart from the data received from the data exporter SPoC, it shall not access other data of the data exporter without data exporter's explicit authorization.

Insofar as compatible with the rules set out in this paragraph as well as in paragraph (d), Exhibit D applies to the processing of personal data by the Supplier.

(d) Any transfer of Personal Data under this Agreement to third countries shall fully comply with the requirements laid down in Chapter V of Regulation (EU) 2018/1725. Any such transfer shall be governed by the AhCCs incorporated in Exhibit A and by its Annexes, insofar as it is not covered by a decision adopted by the European Commission based on Article 45 of Regulation (EU) 2016/679.

For clarity, the Supplier agrees that Exhibit A and its Annexes below, are an integral part of the Agreement and its Amendment. Any obligation on the Processor, as identified in Exhibit A below, is part of the contractual obligations of the Supplier under the Agreement.

(e) The Supplier ensures that specific training procedures for personnel in charge of managing requests for access to personal data from public authorities are in place. These specific training procedures include information on the requirements of EU law as to access by public authorities to personal data and are periodically updated to reflect any new legislative, jurisprudential or other development relevant to the processing of personal data in question."

5) Article 19 of the Agreement is replaced by the following clause:

"The Customer may terminate the Agreement (and/or, for clarity towards the Supplier, any on-going Order Form with the Reseller in connection with the Agreement) in the following circumstances:

(a) if the Supplier is in breach of the data protection obligations of Article 11.2;

(b) if the Supplier does not comply with the applicable data protection obligations resulting from Regulation (EU) 2018/1725;

(c) if the *Ad Hoc Contractual Clauses*, mentioned in Exhibit A, and/or any obligation resulting from these clauses are not being complied with;

(d) where the Customer has evidence that the Supplier or any related entity or person has violated any provisions on security (Article 14 in relation to Exhibit C to this Agreement) and/or confidentiality (Article 18) included in the Agreement.

Termination may either be immediate or enter into force at a date specified by the Customer in the termination notice.

The Customer will apply principles of fairness and reasonableness when considering if to terminate the Agreement.

ARTICLE 2 – MODIFICATION AND ADDITION OF ANNEXES

1. Exhibit A and its Annexes 1a and 1b, as well as Exhibit B, which are attached to this Amendment, are added to the Agreement.

2. Annex 1d to the Agreement is replaced by Exhibit C, attached to this Amendment.

3. Annex 1f to the Agreement is replaced by Exhibit D, attached to this Amendment.

4. Exhibits A and its Annexes 1a and 1b, as well as Exhibits B, C and D form an integral part of the Agreement.

5. All remaining references in the Agreement to Annexes 1d and 1f should be read as references to Exhibits C and D.

ARTICLE 3 - DATE OF ENTRY INTO FORCE

1. This Amendment forms an integral part of the Agreement to which it refers and shall enter into force on the date of signature last written below (the "Amendment Effective Date"), subject to it bearing the signatures of the representatives of the contracting parties.

2. In the event of conflict between the terms of the Agreement and this Amendment the term of this Amendment shall prevail with respect to the subject matter herein.

3. The provisions of the original Agreement that are not modified by the terms of this Amendment shall remain unchanged and shall continue to apply.

ARTICLE 4 - LIST OF ATTACHMENTS TO THIS AMENDMENT

1. Exhibit A "*Ad Hoc* Contractual Clauses" with its
    a. Annex 1a "Cisco Webex Meetings";
    b. Annex 1b "Cisco Technical Assistance (TAC) Service Delivery";
2. Exhibit B "List of Sub-processors";
3. Exhibit C "Information Security Exhibit";
4. Exhibit D "Data Privacy Sheets";

Done at ....., on ..... as an electronic original.

For the Supplier *For the Court of Justice*

EXHIBIT A

***Ad Hoc* Contractual Clauses**[1]

Agreed upon by

1) Data exporter

The data exporter is Customer, acting as data exporter on behalf of itself or a customer where applicable.
Signature and date:

_____

Role: Controller

2) Data importer

The data importer is Cisco Systems, Inc., with registered address at 170 West Tasman Drive, San Jose, California 95134, USA.
Signature and date:

_____

Role: Processor (for Personal Data outside the EEA).

For the purpose of these *ad hoc* contractual clauses (hereinafter: 'Clauses'), a 'Party' is the data exporter or the data importer and the 'Parties' are the data importer and the data exporter.

[1] Based on the model of the new Standard Contractual Clauses for transfers under the GDPR adopted by Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council (O.J. 2021, L 199/31), as applicable to the relationship controller to processor.

SECTION I

Clause 1
Purpose and scope

a. The purpose of these Clauses is to ensure compliance with the requirements of Regulation (EU) 2018/1725 of the European Parliament and the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union Institutions, bodies, offices and agencies and on the free movement of such data for the transfer of personal data to a third country.

b. These Clauses apply with respect to the transfer of personal data as specified in Annexes 1a and 1b of this Exhibit A.

c. The Annexes to this Exhibit A form an integral part of these Clauses.

Clause 2
Effect of the Clauses

a. These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 48(1) and Article 48(3)(a) of Regulation (EU) 2018/1725 and, with respect to data transfers from controllers to processors and/or processors to processors, contractual clauses pursuant to Article 29(3) and (4) of Regulation (EU) 2018/1725. This does not prevent the Parties from including these contractual clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

b. These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2018/1725.

Clause 3
Third-party beneficiaries

a. Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

   i. Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;
   ii. Clause 8, Clause 8.1(b), 8.9(a), (c), (d) and (e);
   iii. Clause 9, Clause 9(a), (c), (d) and (e);
   iv. Clause 12, Clause 12(a), (d) and (f);
   v. Clause 13;
   vi. Clause 15.1(c), (d) and (e);
   vii. Clause 16(e);
   viii. Clause 18, Clause 18(a) and (b).

b. Paragraph (a) is without prejudice to rights of data subjects under Regulation 2018/1725.

Clause 4
Interpretation

a. Where these Clauses use terms that are defined in Regulation (EU) 2018/1725, those terms shall have the same meaning as in that Regulation.

b. These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2018/1725.

c. These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2018/1725.

d. The provisions of Regulation (EU) 2018/1725 follow the same principles as the provisions of Regulation (EU) 2016/679 and should be interpreted homogeneously.

Clause 5
Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6
Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annexes 1a and 1b to this Exhibit A.

Clause 7
Docking clause

a. An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by signing this Exhibit A as well as its Annexes, insofar as these Annexes are relevant to the acceding entity, indicating its agreement to comply with these Clauses as well as with the relevant Annexes to this Exhibit A.

b. Once it has signed this Exhibit A as well as its relevant Annexes, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation as data exporter or data importer.

c. The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8
Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1. Instructions

a. The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

b. The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2. Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annexes 1a and 1b to this Exhibit A, unless on further instructions from the data exporter.

8.3. Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Exhibit C and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 15 and 16 of Regulation (EU) 2018/1725.

8.4. Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5. Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annexes 1a and 1b of this Exhibit A. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6. Security of processing

a. The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter "personal data breach"). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Exhibit C. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

b. The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

c. In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and insofar as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

d. The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2018/1725, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7. Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Exhibit C.

8.8. Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter "onward transfer") if the third party is or agrees to be bound by these Clauses, or if:

a. the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

b. the third party otherwise ensures appropriate safeguards pursuant to Article 48 of Regulation (EU) 2018/1725 with respect to the processing in question;

c. the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

d. the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9. Documentation and compliance

a. The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

b. The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

c. The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

d. The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

e. The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9
Use of sub-processors

a. The data importer has the data exporter's authorisation for the engagement of sub-processors listed in Exhibit B. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through

the addition or replacement of sub-processors at least one (1) month in advance or as early as practically possible (if so), thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

b. Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

c. The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

d. The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

e. The data importer shall agree a third-party beneficiary clause with the sub-processor whereby - in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent - the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

f. The use of sub-processors is, in case of any onward transfer of personal data, subject to a contract being signed between the data importer and the sub-processor, or, as the case may be, between a sub-processor and a sub-processor, which includes the appropriate Standard Contractual Clauses adopted by the Commission on the basis of Article 46(2)(c) of Regulation (EU) 2016/679 as well as, in addition, a provision that these Standard Contractual Clauses prevail over any other contractual obligation between the data importer and the sub-processor or, as the case may be, between a sub-processor and a sub-processor. This contract (referred to in this paragraph f.) may, where applicable, take the form of an intra-group agreement. The sub-processor shall apply technical and organisational measures that, at least, reach the same level of security as those mentioned in Exhibit C.

g. Paragraph (f) also applies in case of an onward transfer of personal data to any affiliate or partner of the data importer or a sub-processor.

Clause 10
Data subject rights

a. The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

b. The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2018/1725. In this regard, the Parties shall set out in Exhibit C the

appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

c. In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11
Redress

a. The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

b. In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

c. Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

   i. lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

   ii. refer the dispute to the competent courts within the meaning of Clause 18

d. The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679 or Article 67 of Regulation (EU) 2018/1725.

e. The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

f. The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12
Liability

a. Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

b. The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

c. Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter under Regulation (EU) 2018/1725.

d. The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

e. Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

f. The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage.

g. The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13
Supervision

a. The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2018/1725 as regards the data transfer, as indicated in Annexes 1a and 1b to this Exhibit A, shall act as competent supervisory authority.

b. The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14
Local laws and practices affecting compliance with the Clauses

a. The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679 or Article 25(1) of Regulation (EU) 2018/1725, are not in contradiction with these Clauses.

b. The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

    i. the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the

purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

ii. the laws and practices of the third country of destination – including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;

iii. any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

c. The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

d. The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

e. The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

f. Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g.: technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

15.1. Notification

a. The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary, with the help of the data exporter) if it:

i. receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

ii. becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

b. If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

c. Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

d. The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

e. Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2. Review of legality and data minimisation

a. The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

b. The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

c. The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16
Non-compliance with the Clauses and termination

a. The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

b. In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

c. The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

   i. the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

   ii. the data importer is in substantial or persistent breach of these Clauses; or

   iii. the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

   In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

d. Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

e. Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725.

Clause 17
Governing law

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of the Grand Duchy of Luxembourg.

Clause 18
Choice of forum and jurisdiction

a. Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State or, in the case of exclusive jurisdiction, by the Court of Justice of the European Union.

b. The Parties agree that, in the case of jurisdiction of the courts of an EU Member State, those shall be the courts of the Grand Duchy of Luxembourg.

c. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence, except for issues for which the Court of Justice of the European Union has exclusive jurisdiction.

d. The Parties agree to submit themselves to the jurisdiction of such courts.

ANNEX 1a TO EXHIBIT A

CISCO WEBEX MEETINGS: Transfers of Personal Data

This Annex 1a "Cisco Webex Meetings" forms an integral part of the *Ad Hoc* Contractual Clauses in Exhibit A and describes transfers of personal data outside of the EEA associated with use of Cisco Webex Meetings (the "Service" or "Webex Meetings"). This Annex intends to describe the current state of those transfers.

The data importer informs the data exporter of any update in the processing operations detailed in this Annex 1a in accordance with paragraph (c) of Article 1 of this Amendment. Any such update fully complies with the requirements laid down in Regulation (EU) 2018/1725 and, in particular, in its Chapter V, as well as with the *Ad Hoc* Contractual Clauses in Exhibit A.

A. Description of transfer

1. Categories of data subjects whose personal data is transferred

The personal data transferred may concern the following categories of data subjects: Employees, contractors, business partners, representatives and end customers of the Customer, and other individuals whose personal data is processed by or on behalf of Customer or Customer's customers and delivered as part of the Services and Products.

2. Categories of personal data transferred

Personal data category	Types of personal data
User Information	• Name • Email Address • Password • Browser • Phone Number (Optional) • Mailing Address (Optional) • Avatar (Optional) • User Information Included in Your Directory (if synched) • Unique User ID (UUID) (a pseudonymized 128-bit number assigned to compute nodes on a network)
Host and Usage Information	• IP Address • User Agent Identifier • Hardware Type • Operating System Type and Version • Client Version • IP Addresses Along the Network Path • MAC Address of Your Client (As • Applicable) • Service Version • Actions Taken • Geographic Region

	• Meeting Session Information (e.g., date and time, frequency, average and actual duration, quantity, quality, network activity, and network connectivity) • Number of Meetings • Number of Screen-Sharing and NonScreen-Sharing Sessions • Number of Participants • Screen Resolution • Join Method • Performance, Troubleshooting, and Diagnostics Information • Meeting Host Information (Host Name and ID, Meeting Site URL and Meeting Start/End Time) • Meeting Title • Call attendee information, including email addresses, IP address, username, phone numbers, room device information • Information submitted through attendee registration form (Optional)
User-Generated Information	• Meeting Recordings (if enabled by Customer) • Transcriptions of meeting recordings (optional, only applicable if enabled by you) • Uploaded Files (for WebEx Events and Training only)

3. Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

Unless data exporter or its users use data importer's products and services to transmit or store sensitive data, data importer does not process sensitive data.

4. The frequency of the transfer (e.g.: whether the data is transferred on a one-off or continuous basis).

The Transfer happens on a continuous basis during the provisioning and use of the Service.

5. Nature of the processing

Webex Meetings is a cloud-based web and video conferencing solution made available by Cisco to companies or persons who acquire it for use by their authorized users (each, a "user"). The Service enables global employees and virtual teams to collaborate in real time from anywhere, anytime, on mobile devices or video systems as though they were working in the same room. Solutions include meetings, events, training, and support services. For more information regarding optional features for Cisco Webex Meetings, please see the Addendums below.

Because the Service enables collaboration among its users, as described below, your personal data is required in order to use the Service. Additionally, given the global nature of the Service, some transfers of data outside of the EU/EEA do occur.

Cisco Webex Meetings has implemented the following appropriate technical and organizational measures designed to secure personal data from accidental loss and unauthorized access, use, alteration, and disclosure, including during transfers of personal data.

Encryption of data in transit

All communications between cloud registered WebEx Apps, WebEx Room devices and WebEx services occur over encrypted channels. WebEx uses the TLS protocol with version 1.2 or later with high strength cipher suites for signalling.

After a session is established over TLS, all media streams (audio VoIP, video, screen share, and document share) are encrypted.

Encrypted media can be transported over UDP, TCP, or TLS. Cisco prefers and strongly recommends UDP as the transport protocol for WebEx voice and video media streams. This is because TCP and TLS are connection orientated transport protocols, designed to reliably deliver correctly ordered data to upper-layer protocols. Using TCP or TLS, the sender will retransmit lost packets until they are acknowledged, and the receiver will buffer the packet stream until the lost packets are recovered. For media streams over TCP or TLS, this behaviour manifests itself as increased latency/jitter, which in turn affects the media quality experienced by the call's participants.

Media packets are encrypted using either AES 256 or AES 128 based ciphers. The WebEx App and WebEx Room devices uses AES-256-GCM to encrypt media; these media encryption keys are exchanged over TLS-secured signalling channels. SIP and H323 devices that support media encryption with SRTP can use AES-256-GCM, AES-128-GCM, or AES-CM-128-HMAC-SHA1 (AES-256-GCM is the WebEx preferred media encryption cipher).

Zero Trust Security Based End-to-End Encryption for Webex Meetings

For standard WebEx Meetings, where devices and services use SRTP to encrypt media on a hop by hop basis, Webex media servers need access to the media encryption keys to decrypt the media for each SRTP call leg. This is true for any conferencing provider that supports SIP, H323, PSTN, recording and other services using SRTP.

However, for businesses requiring a higher level of security, WebEx also provides end-to-end encryption for meetings ("Webex Zero Trust Security end-to-end encryption"). With this option, the WebEx cloud does not have access to the encryption keys used by meeting participants and cannot decrypt their media streams. WebEx Zero Trust Security end-to-end encryption uses standard track protocols to generate a shared meeting encryption key (Messaging Layer Security (MLS)) and to encrypt meeting content (Secure Frame (S-Frame). With MLS, the meeting encryption key is generated by each participant's device using a combination of the shared public key of every participant and the participant's private key (never shared). The meeting encryption key does not traverse the cloud and is rotated as participants join and leave the meeting. For more details on Zero Trust Security based end-to-end encryption see the Zero Trust Security for WebEx white paper.

With end-to-end encryption, all meeting content (voice, video, chat, etc.) is encrypted using the locally derived meeting encryption key. This data cannot be deciphered by the WebEx service.

Note that when end-to-end encryption is enabled, WebEx services and endpoints that need access to meeting keys to decrypt content (e.g.: devices using SRTP where encryption is performed hop by hop) are not supported. This restricts meeting participants to those using the WebEx App or cloud registered WebEx devices only, and excludes services such as network-based recording, speech recognition etc. The following features are also not supported:

- Join Before Host
- Video-device enabled meetings
- Linux clients
- Network-Based Recording (NBR)
- WebEx Assistant
- Saving session data transcripts, Meeting Notes

(i) PSTN Call-in/Call-back

6. Purpose(s) of the data transfer and further processing

Cisco has implemented Webex Data Residency for EU customers. Webex data residency provides Customer user administrators the ability to choose where their organization's data is stored, in particular personal data processed by Webex Meetings, including User Information, Host & Usage Information, and User-Generated Information (other than as noted below). For those EU Customers that became Webex Meetings Customers after July 2021, data is by default stored where those Customers are provisioned. For EU Customers who were provisioned before July 2021, user administrators will be provided instructions on how to migrate their user data, through Control Hub, to the location where they are provisioned. Data associated with the CJEU has already been migrated to the EU. To facilitate certain operations and aspects of the Service, certain exceptions to Webex Data Residency exist, which are described below:

Data transfers outside of the EU/EEA may take place for the following reasons: (a) a user registers on any Cisco platform (for example, through www.webex.com or www.cisco.com) or through any Cisco service to learn more about Cisco products or events; (b) a Customer provides ordering information (business contact information); (c) a user engages in collaboration with users outside of the EU region; (d) a user requests technical support through Cisco's Technical Assistance Center ("TAC") (in which case the information that a user provides within the initial TAC request may be transferred outside region); (e) a user enables certain optional functionalities; or (f) a user enables cell phone "push" notifications (in which case the cell phone provider associated with iOS or Android functionality may transfer data outside of the region).

Personal Data Category	Types of Data	Purpose of data transfer and further processing
User Information	• Name • Email Address • Password • Browser • Phone Number (Optional) • Mailing Address (Optional) • Avatar (Optional) • User Information Included in Your Directory (if synched) • Unique User ID (UUID) (a pseudonymized 128-bit number assigned to compute nodes on a network)	Transfers of User Information only occur in certain scenarios, as identified above.

Host and Usage Information	• IP Address • User Agent Identifier • Hardware Type • Operating System Type and Version • Client Version • IP Addresses Along the Network Path • MAC Address of Your Client (As • Applicable) • Service Version • Actions Taken • Geographic Region • Meeting Session Information (e.g., date and time, frequency, average and actual duration, quantity, quality, network activity, and network connectivity) • Number of Meetings • Number of Screen-Sharing and Non-Screen-Sharing Sessions • Number of Participants • Screen Resolution • Join Method • Performance, Troubleshooting, and Diagnostics Information • Meeting Host Information (Host Name and ID, Meeting Site URL and Meeting Start/End Time) • Meeting Title • Call attendee information, including email addresses, IP address, username, phone numbers, room device information • Information submitted through attendee registration form (Optional)	Transfers of Host & Usage Information only occur in certain scenarios, as identified above.

User-Generated Information	• Meeting Recordings (if enabled by Customer) • Transcriptions of meeting recordings (optional, only applicable if enabled by you) • Uploaded Files (for Webex Events and Training only	Transfers of User-Generated Information only occur in certain scenarios, as identified above.

In the specific case of sub-processors, purposes of data transfers and further processing are explained in Exhibit B.

7. The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

Subject to their employer's corporate retention policies, users with an active subscription can delete User-Generated Information from their account through the My WebEx Meetings page at any time during the term of their subscription.[2] Enterprise Customers have the ability to set organization-wide retention periods for recordings using APIs. Cisco provides free account users up to 6 months of free storage.

The table below lists the personal data used by Cisco Webex Meetings, the length of time that data needs to be retained, and why we retain it.

Users seeking deletion of User Information and User Generated Information retained on their employer's Webex Meetings site must request deletion from their employer's site administrator.

[2] Recordings are soft-deleted and will be retained on the platform for 30 days after user deletion, in the event the Customer or user inadvertently deletes the recording and seeks to restore.

Personal Data category	Retention period	Reason and criteria for retention
User Information	Active Subscriptions: User Information will be maintained as long as Customer maintains active subscription (paid or free). Terminated Service: • Deleted once the Service is terminated • Name and UUID are maintained seven (7) years from termination	Name and UUID are maintained seven (7) years from termination as part of Cisco's business records and are maintained to comply with Cisco's financial and audit requirements. Any billing information is also subject to this retention period.
User-Generated Information	Active Subscriptions: At Customer's or user's discretion Terminated Service: Deleted within sixty (60) days	User-Generated Information, except for recordings, is not retained on the Webex Meetings platform when Customer or user deletes this data. Recordings are "soft deleted" and retained for 30 days before being removed from the platform, to allow a Customer or user to retrieve a recording they have inadvertently deleted. User Generated Information is retained for 60 days after services are terminated to give Customers opportunity to download.
Host and Usage Information	Three (3) years from when the Service is terminated	Host and Usage is kept as part of Cisco's record of Service delivery. * Any billing information is retained for 7 years as part of Cisco's business records and are maintained to comply with Cisco's financial and audit requirements. Once the specified retention period has expired, data will be deleted.

8. For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

See Exhibit B.

B. Competent Supervisory Authority

The European Data Protection Supervisor, established by Article 52(1) of Regulation (EU) 2018/1725.

C. Additional commitments

1. The data importer certifies with regard to the ELA Cloud Services being free of functions that may affect Personal Data integrity, confidentiality, and availability that the data importer has not intentionally:

i. created certain programming functions that could be used to access, transmit or send the Personal Data without authorization from the Customer,

ii. created or changed its operational processes regarding Processing of Personal Data in a manner that facilitates access/change/manipulation to Personal Data other than authorized under the Agreement and its Exhibits, and

iii. created or maintained programming functions designed to facilitate access by a public authority to Personal Data .

2. The data importer certifies that:

i. it does not access the data of the data exporter by default (i.e., without a support request).

ii. it will provide remote TAC only in case a Single Point of Contact (SPoC) from the data exporter makes a formal request, in which case it will be provided manually with the minimum amount of anonymized data needed for the resolution of the problem, and

iii. apart from the data received from the data exporter SpoC, it shall not access other data of the data exporter without data exporter's explicit authorization.

3. The data importer ensures that specific training procedures for personnel in charge of managing requests for access to personal data from public authorities are in place. These specific training procedures include information on the requirements of EU law as to access by public authorities to personal data and are periodically updated to reflect any new legislative, jurisprudential or other development relevant to the transfer of personal data in question.

Annex 1b To Exhibit A

CISCO TECHNICAL ASSISTANCE (TAC) SERVICE DELIVERY: Transfers of Personal Data

This Annex 1b "TAC Support Information" forms an integral part of the *Ad Hoc* Contractual Clauses in Exhibit A.

The data importer informs the data exporter of any update in the processing operations detailed in this Annex 1b in accordance with paragraph (c) of Article 1 of this Amendment. Any such update fully complies with the requirements laid down in Regulation (EU) 2018/1725 and, in particular, in its Chapter V, as well as with the *Ad Hoc* Contractual Clauses in Exhibit A.

A. Description of transfer

1. Categories of data subjects whose personal data is transferred

The personal data transferred may concern the following categories of data subjects: Employees, contractors, business partners, representatives and end customers of the Customer, and other individuals whose personal data is processed by or on behalf of Customer or Customer's customers and delivered as part of the Services and Products.

2. Categories of personal data transferred

The personal data transferred may concern the following categories of data:

Personal data category	Types of personal data
TAC Support Information	• Name • Email Address • Phone Number of the Employee Appointed to Open the Service Request • Authentication Information (exclusive of passwords) • Work organization and responsibilities • Current employer name
Customer Case Attachment	Cisco TAC does not intentionally collect or process personal data via Customer Case Attachments. We instruct customers to provide the least amount of personal data possible. However, unsolicited personal data may be contained in the files provided by customers. For illustrative purposes only, the list below includes the types of data that may be processed for Customer Case Attachments for the purpose of providing support: •Device Configuration (e.g., running config and startup config, SNMP Strings (masked); Interface description • Command Line Interface (CLI) (i.e., Show Commands, such as Show Version) •Product Identification Numbers • Serial Numbers • Host Names •Sysdescription (has device location) • IP Addresses • Operating System (OS) Feature Sets

	• OS Software Versions • Hardware Versions • Installed Memory • Installed Flash • Boot Versions • Chassis Series • Slot IDs • Card Types • Card Families • Firmware Versions • MAC Address • SNMP MIBs (ACLs, CDP)

*WebEx Meetings' User Information and Host and Usage Information (see section 2 of Annex 1a above) are also transferred to provide TAC support.

3. Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

Unless data exporter or its users use data importer's products and services to transmit or store sensitive data, data importer does not process sensitive data.

4. The frequency of the transfer (e.g.: whether the data is transferred on a one-off or continuous basis).

The transfer happens only when a support ticket is opened.

5. Nature of the processing

Data importer's Support Services Technical Assistance Center (TAC) is a global organization that provides around-the clock, award-winning technical support services online and over the phone. TAC offers customer support for all data importer's products/services using a global follow-the-sun support model. .

As part of TAC services support process, service requesters may be required to provide certain personal data, that will be transferred as needed in order to provide the support services. These data are limited to business contact details provided by the requester and used for the purposes of providing the support required.

Additionally, Cisco has implemented the following appropriate technical and organizational measures designed to secure personal data from accidental loss and unauthorized access, use, alteration, and disclosure when transferred to third countries.

Personal data category	Security controls and measures
TAC Support Information	• Data encryption, in transit • Authentication • Access control • Login/activity logging and monitoring • Data masking
Customer Case Attachment	• Data encryption, both at rest and in transit • Authentication • Access control • Login/activity logging and monitoring • Data masking • Transport and storage for physical data

6. Purpose(s) of the data transfer and further processing

TAC leverages a Customer Relationship Management (CRM) case management system to deliver services and capture TAC Support Information. This system is a customized instance on the SalesForce.com (SFDC) platform known as Support Case Manager (SCM) and utilizes a numerical Service Request (SR) case assignment process TAC SR case details and associated case notes within data importer's CRM system are stored at the Salesforce.com (SFDC) data center, which physically resides in Washington DC, USA.

Customer Case Attachments (including detailed system logs, etc.) uploaded by customers are housed in a single data repository hosted by Amazon Web Services (AWS -US East, North Virginia Region). The AWS instance, known internally as CX Files, maintains robust data security and governance controls, including authentication, authorization, role-based access controls, encryption in transit and at rest, login logging and monitoring, and activity logging and monitoring. CX Files is wholly maintained by the Cisco Customer Care IT / Crypto team and the storage location is not shared with any other AWS customers, nor with any other team within data importer.

Additionally, the following are the Cisco entities located in third countries not covered by an adequacy decision, taking part in TAC support:[3]

Cisco Systems Private Limited (India) – CapGemini
Cisco - Estarta (Jordan)
Cisco Systems, Inc (USA)

[3] Other Cisco entities taking part in TAC support are the following: Cisco Systems, Inc (Belgium), Cisco Systems International BV (Netherlands), Cisco Systems (Bulgaria), Cisco Systems (Poland), Cisco International Limited (Portugal) and Cisco International Limited (UK).

All these entities employ TAC engineers who participate in personal and other data processing within full SR lifecycle. All these entities have signed Cisco's Intragroup agreement which includes the Processor-to-Processor module of the Standard Contractual Clauses.

For ease of reference and further conversation on other sub-processors involved, we should distinguish between TAC Support information and Customer Case Attachment, as stated above.

TAC Support information is hosted on SFDC instance (Washington DC, USA). This information is encrypted in transit. Salesforce.com is a sub-processor in this instance. Personal data in question is Business personal data (as per table in section 2 above) of end users who will be opening the case.

On the other hand, Customer Case Attachments are hosted on Amazon Web Services (US – East Region, Northern Virginia – replicated to Oregon). Case attachments are encrypted both in transit and at rest. AWS qualifies as a sub-processor in this instance. All these Case Attachments are unstructured data types in form of logs over which customer has a degree of control.

Infrastructure Provider Locations
Amazon Web Services (AWS) – US East (Northern Virginia) Region
Amazon Web Services (AWS) – US West (Oregon) Region
SalesForce.com (SFDC) – Washington D.C., USA

7. The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

TAC Service Request (SR) case data that has been in CLOSED status for 10 years + 1 day or more is automatically purged from our key repositories on a nightly basis. Case data is all data captured as part of the service request process, including all TAC Support Information and Customer Case Attachments. This information is retained to ensure efficient support in case of recurring issues and to comply with Cisco audit policies related to business records of services provided to customers (i.e., legitimate business purposes).

Data exporter can request deletion of personal data retained by TAC by submitting a request via privacy portal. If data exporter requires deletion of any other data outside of the timelines stated above, it has to contact its sales representative. In each instance, data importer will endeavor to delete the requested data from its systems at the earliest possible time and will do so unless the data is required to be retained by data importer.

8. For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

See Exhibit B.

B. Competent Supervisory Authority

The European Data Protection Supervisor, established by Article 52(1) of Regulation (EU) 2018/1725.

C. Additional commitments

1. The data importer certifies with regard to the ELA Support being free of functions that may affect the Personal Data integrity, confidentiality and availability, that has not intentionally:

   i. created certain programming functions that could be used to access, transmit or send the Personal Data without authorization from the Customer,

   ii. created or changed its operational processes regarding Processing of Personal Data in a manner that facilitates access/change/manipulation to the Personal Data other than authorized under the Agreement and its Exhibits, and

   iii. created or maintained programming functions designed to facilitate access by a public authority to Personal Data.

2. The data importer certifies that:

   i. It does not access the data of the data exporter by default (i.e., without a support request).

   ii. it will provide remote TAC only in case a Single Point of Contact (SPoC) from the data exporter makes a formal request, in which case it will be provided manually with the minimum amount of anonymized data needed for the resolution of the problem, and

   iii. apart from the data received from the data exporter SPoC, it shall not access other data of the data exporter without data exporter's explicit authorization.

3. The data importer ensures that specific training procedures for personnel in charge of managing requests for access to personal data from public authorities are in place. These specific training procedures include information on the requirements of EU law as to access by public authorities to personal data and are periodically updated to reflect any new legislative, jurisprudential or other development relevant to the transfer of personal data in question.

Exhibit B

List of Sub-processors

The controller has authorised the use of the following sub-processors:

- Cisco TAC

Sub-processor	Personal Data	Service Type under the Agreement and purpose of processing	Location	Official Address
Salesforce.com (USA)	TAC Support Information	Hosting/Storage	Washington, DC, USA	415 Mission Street, 3rd Floor, San Francisco, CA 94105
Amazon Web Services, Inc (USA)	Customer Case Attachments	Hosting/Storage	Northern Virginia and Oregon, USA	410 Terry Avenue North Seattle, WA 98109-5210
Cisco Systems, Inc (Belgium)	TAC Support Information, Customer Case Attachments	Provision of TAC Services	Belgium	Pegasus Park De Kleetlaan 6A Diegem, 1831 Belgium
Cisco -Estarta	TAC Support Information, Customer Case Attachments	Provision of TAC Services	Jordan	Jubelha, Queen Rania Street, P.O. Box 941934 Amman 11194 Jordan
Cisco Systems International BV (The Netherlands)	TAC Support Information, Customer Case Attachments	Provision of TAC Services	The Netherlands	Haarlerbergpark, Haarlerbergweg 13-19, 1101-CH Amsterdam, The Netherlands
Cisco Systems (Bulgaria) - IBM	TAC Support Information, Customer Case Attachments	Provision of TAC Services	Bulgaria	Cisco Systems Bulgaria EOOD, Business Park Sofia, Building 11B, floor 4, 1766 Sofia, Bulgaria
Cisco Systems (Poland)	TAC Support Information, Customer Case Attachments	Provision of TAC Services	Poland	Ul. Powstańców Wielkopolskich 13 c Kraków, małopolskie, 30-707 Poland
Cisco Systems Private Limited (India) - CapGemini	TAC Support Information, Customer Case Attachments	Provision of TAC Services	India	SEZ Unit, Cessna Business Park, Kadubeesanahalli Village, Hobli, Sarjapur, Varthur Rd, Marathahalli, Bengaluru, Karnataka 560103, India

- Cisco Webex Meetings

Subprocessor	Personal Data	Service Type under the Agreement and purpose of processing	Location	Official address
Akamai Technologies, Inc.	IP address, Browser and Geographic region	Akamai is used as content delivery network (CDN) services provider for static content. Akamai does not store content but may store IP address in logs for a maximum of 3 years.	Location generally maps to Customer's Webex data center assignment. To the extent Akamai receives IP addresses of Webex Meeting customers, those IP addresses may be transmitted to the United States with strict access control means and appropriate safeguards under the EU Standard Contractual Clauses (SCCs).	3715 Northside Parkway, N.W.. Bldg. 200, Suite 300. Atlanta, GA 30327
Amazon Web Services, Inc. (AWS)	Limited Host & Usage Information	AWS cloud infrastructure is used to host the WebEx signaling service that processes real-time meeting lifecycle information such as meeting participant UUIDs, meetings start and end times. Data will be deleted within 15 days of the meeting. (location maps to Customer's WebEx data center assignment) AWS cloud infrastructure is used to host WebEx media nodes that may process real-time meeting data such as VoIP, video and high frame rate sharing data. This information is not retained in AWS once your meeting has ended.	United States Germany Netherlands United Kingdom Brazil Australia Japan Singapore	410 Terry Avenue North Seattle, WA 98109-5210
WalkMe, Inc.* * Customers may turn this feature off at any time.	Unique User ID (UUID) and user region	Provides user with a step-by-step tour and guidance on how to use WebEx Meetings online site.	United States	71 Stevenson St floor 20, San Francisco, CA 94105

Feature is currently enabled for non-enterprise WebEx sites.				
Vbrick (WIP)	Name, UUID, email address	Vbrick provides users with extended capacity for WebEx Meetings including over 3,000 participants. Vbrick requires the data for authentication and the data is encrypted in transit.	United States EU: Germany, Ireland Australia	2121 Cooperative Way Suite 100 Herndon, VA 20171 United States

Exhibit C

Information Security Exhibit

1. Scope

This document describes the technical and organizational security measures that shall be implemented by Cisco to secure Personal Data, Customer Content and Systems Information (collectively, "Data") prior to any processing under the Agreement.

2. General Security Practices

Cisco has implemented and shall maintain appropriate technical and organizational measures designed to protect Data against accidental loss, destruction or alteration, unauthorized disclosure or access, or unlawful destruction, including the policies, procedures, and internal controls set forth in this document for its Representatives, facilities, and equipment at Cisco's locations involved in Cisco's performance of its obligations under the Agreement.

3. General Compliance

3.1. **Compliance.** Cisco shall document and implement processes to avoid breaches of legal, statutory, regulatory, or contractual obligations related to information security or other security requirements. Such processes shall be designed to provide appropriate security to protect Data given the risk posed by the nature of the Data processed by Cisco. Cisco shall implement and operate information security in accordance with Cisco's own policies, which shall be no less strict than the information security requirements set forth in this document.

3.2. **Protection of logs and records.** Cisco shall implement appropriate procedures designed to protect logs and records from loss, destruction, falsification, unauthorized access, and unauthorized release, in accordance with legislative, regulatory, and contractual requirements.

3.3. **Review of information security.** Cisco's approach to managing information security and its implementation shall be reviewed at planned intervals or when significant changes occur by appropriate internal or external assessors.

3.4. **Compliance with security policies and standards.** Cisco's management shall regularly review the compliance of information processing and procedures with the appropriate applicable security policies and standards.

3.5. **Technical compliance review.** Cisco shall regularly review information systems for compliance with Cisco's information security policies and standards.

3.6. **Information Risk Management ("IRM").** Cisco shall implement and utilize an appropriate information risk management process to frame, assess, respond and monitor risk, consistent with applicable contractual and legal obligations. Threat and vulnerability assessments must be reviewed periodically and prompt remediation actions taken where material weaknesses are found.

3.7. **Processing of Sensitive Personal Data.** To the extent that Cisco processes Sensitive Personal Data and the security measures referred to in this document are deemed to provide insufficient protection, Customer may request that Cisco implement additional security measures.

4. Technical and Organizational Measures for Security

4.1. Organization of Information Security

a. **Security Ownership.** Cisco shall appoint one or more security officers responsible for coordinating and monitoring the security requirements and procedures. Such officers shall have the knowledge, experience, and authority to serve as the owner(s) of, with responsibility and accountability for, information security within the organization.

b. **Security Roles and Responsibilities.** Cisco shall define and allocate information security responsibilities in accordance with Cisco's approved policies for information security. Such policies (or summaries thereof) shall be published and communicated to employees and relevant external parties required to comply with such policies.

c. **Project Management.** Cisco shall address information security in project management to identify and appropriately address information security risks.

4.2. Human Resources Security

a. **General.** Cisco shall ensure that its personnel are subject to confidentiality obligations and shall provide adequate training about relevant privacy and security policies and procedures. Cisco shall further inform its personnel of possible consequences of breaching Cisco's security policies and procedures, which must include disciplinary action, including possible termination of employment for Cisco's employees and termination of contract or assignment for relevant external Representatives (e.g., contractors, agents, consultants etc.).

b. **Training.** Representatives with access to Data shall receive appropriate, periodic (i.e., at least annual) education and training regarding privacy and security procedures to aid in the prevention of unauthorized use (or inadvertent disclosure) of Data and training regarding how to effectively respond to security incidents. Training shall be provided before Representatives are granted access to Data or begin providing Services. Training shall be regularly reinforced through refresher training courses, emails, posters, notice boards, and other training and awareness materials.

c. **Background Checks.** Cisco shall require criminal and other relevant background checks for Representatives in compliance with mandatory applicable law and Cisco's policies.

4.3. Access Controls

a. **Access**.

i. Limited Use. Cisco will not (i) access the Customer's computer systems for any purpose other than as necessary to perform its obligations under the Agreement or as otherwise agreed to by the parties; or (ii) use any system access information or log-in credentials to gain unauthorized access to Data or

Customer's systems, or to exceed the scope of any authorized access.

ii. Authorization. Cisco shall restrict access to Data and systems at all times solely to those Representatives whose access is necessary.

iii. Suspension or Termination of Access Rights. At Customer's reasonable request, Cisco shall promptly and without undue delay suspend or terminate the access rights to Data and systems for any Representatives reasonably suspected of breaching any of the provisions of this document; and Cisco shall remove access rights of all Cisco employees and relevant external parties upon suspension or termination of their employment or engagement.

iv. Information Classification. Cisco shall classify, categorize, and/or tag Data to help identify it and to allow for access and use to be appropriately restricted.

b. Access Policy. Cisco shall determine appropriate access control rules, rights, and restrictions for each specific user's roles towards their assets. Cisco shall maintain a record of security privileges of Representatives that have access to Data, networks, and network services. Cisco shall restrict the use of utility programs that might be capable of overriding system and application controls.

c. Access Authorization

i. Cisco shall have user account creation and deletion procedures, with appropriate approvals, for granting and revoking access to its systems and networks. Cisco shall use an enterprise access control system that requires revalidation of Representatives by managers at regular intervals based on the principle of "least privilege" and need-to-know criteria based on job role.

ii. Cisco shall maintain and update a record of its users authorized to access systems that contain Data and Cisco shall review such users' access rights at regular intervals.

iii. For systems that process Data, Cisco shall revalidate (or where appropriate, deactivate) access of Representatives who change Cisco reporting structure and deactivate authentication credentials that have not been used for a period of time not to exceed six (6) months.

iv. Cisco shall restrict access to program source code and associated items such as software object code, designs, specifications, verification plans, and validation plans, to prevent the introduction of unauthorized functionality and to avoid unintentional changes.

d. Network Design. For systems that process Data, Cisco shall have controls to avoid Representatives assuming access rights that could be used to gain unauthorized access to Data.

e. Least Privilege. Cisco shall limit Representatives' access to Data to those Representatives who have an actual need to access such Data to perform their assigned duties.

f. Authentication

i. Cisco shall use industry standard practices including ISO/IEC 27002:2013 and NIST SP 800- 63B (Digital Identity Guidelines) to identify and authenticate users who attempt to access information systems.

ii. Where authentication mechanisms are based on passwords, Cisco shall require the password to conform to strong password control parameters (e.g., length, character complexity, and/or non-repeatability) with at least 8 characters and containing the following four classes: upper case, lower case, numeral, special character.

iii. Cisco shall maintain industry standard procedures to prevent de-activated or expired identifiers and log-in credentials from being granted to other individuals.

iv. Cisco shall monitor repeated failed attempts to gain access to its information systems.

v. Cisco shall maintain industry standard procedures to deactivate log-in credentials that have been corrupted or inadvertently disclosed.

vi. Cisco shall use industry standard log-in credential protection practices, including practices designed to maintain the confidentiality and integrity of log-in credentials when they are assigned and distributed, and during storage (e.g., log-in credentials shall not be stored or shared in plain text). Such practices shall be designed to ensure strong, confidential log-in credentials.

vii. Cisco shall implement a multi-factor authentication solution to authenticate Representatives accessing its information systems.

4.4. Physical and Environmental Security

a. Physical Access to Facilities

i. Cisco shall limit access to facilities where systems that process Data are located to authorized individuals.

ii. Security perimeters shall be defined and used to protect areas that contain both sensitive or critical information and information processing facilities.

iii. Facilities shall be monitored and access-controlled at all times (24x7).

iv. Access shall be controlled through key card and/or appropriate sign-in procedures for facilities with systems processing Data. Cisco must register authorized individuals and require them to carry appropriate identification badges.

b. Physical Access to Equipment. Cisco equipment used to process Data shall be protected using industry standard processes to limit access to authorized Representatives.

c. Protection from Disruptions. Cisco shall implement appropriate measures designed to protect against loss of data due to power supply failure or line interference.

d. Clear Desk. Cisco shall have policies requiring a "clean desk/clear screen" designed to prevent inadvertent disclosure of Data.

4.5. Operations Security

a. Operational Policy. Cisco shall maintain written policies describing its security measures and the relevant procedures and responsibilities of Representatives who have access to Data and to its systems and networks. Cisco shall communicate its policies and requirements to all Representatives involved in the processing of Data. Cisco shall implement the appropriate management structure and control designed to maintain compliance with such policies and with mandatory applicable law concerning the protection and processing of Data.

b. Security and Processing Controls.

i. **Areas.** Cisco shall maintain, document, and implement standards and procedures to address the configuration, operation, and management of systems and networks that process Data.

ii. **Standards and Procedures.** Such standards and procedures shall include security controls, identification and patching of security vulnerabilities, change control process and procedures, and incident prevention, detection, remediation, and management.

c. Logging and Monitoring. Cisco shall maintain logs of administrator and operator activity and data recovery events related to Data.

4.6. Communications Security and Data Transfer

a. Networks. Cisco shall, at a minimum, use the following controls to secure its corporate networks that process Data:

i. Network traffic shall pass through firewalls, which are monitored at all times. Cisco must implement intrusion detection systems and/or intrusion prevention systems.

ii. Anti-spoofing filters and controls must be enabled on routers.

iii. Network, application, and server authentication passwords are required to meet the same industry standard practices used for the authentication of users set forth in Section 4.3.f above (Authentication). System-level passwords (privileged administration accounts or user- level accounts with privileged administration access) must be changed at minimum every 90 days.

iv. Initial user passwords are required to be changed at first log-on. Cisco shall have a policy prohibiting the sharing of user IDs, passwords, or other log-in credentials.

v. Firewalls must be deployed to protect the perimeter of Cisco's networks.

b. Virtual Private Networks ("VPN"). When using VPN to remotely connect to the Customer's or Cisco's network for processing of Data:

i. Connections must be encrypted using industry standard cryptography.

ii. Connections shall only be established using VPN servers.

iii. The use of multi-factor authentication is required.

c. Data Transfer. Cisco shall have formal transfer policies in place to protect the transfer of Data through the use of all types of communication facilities that adhere to the requirements of this document. Such policies shall be designed to protect transferred Data from unauthorized interception, copying, modification, corruption, routing and destruction.

4.7. System Acquisition, Development, and Maintenance

a. Security Requirements. Cisco shall adopt security requirements for the purchase, use, or development of information systems, including for application services delivered through public networks.

b. Development Requirements. Cisco shall have policies for secure development, system engineering, and support. Cisco shall conduct appropriate tests for system security as part of acceptance testing processes. Cisco shall supervise and monitor the activity of outsourced system development.

4.8. Penetration Testing and Vulnerability Scanning & Audit Reports

a. **Testing.** Cisco will perform periodic vulnerability scans and penetration tests on its internet perimeter network. These scans and tests will be conducted by qualified professionals, includingamong other entities,

Cisco's independent internal compliance team, using industry standard tools and methodologies.

b. **Audits and Certifications.** Cisco shall cooperate with reasonable requests by Customer for legally required security audits (subject to mutual agreement on the time, duration, place, scope and manner of the audit), and respond to reasonable requests for testing reports. Cisco shall make available to Customer, upon written request and without undue delay, copies of any third party audit reports or certifications it maintains (such as SSAE 16 – SOC1, SOC2, SOC3 attestations or ISO 27001:2013 certifications (or their equivalent under any successor standards)) that apply to the Service, to the extent that Cisco maintains such certifications in its normal course of business. Customer shall treat the contents of reports related to Cisco's security and certifications as confidential information.

c. **Remedial Action.** If any penetration test or vulnerability scan referred to in Section 4.8.a above reveals any deficiencies, weaknesses, or areas of non-compliance, Cisco shall promptly take such steps as may be required, in Cisco's reasonable discretion, to address material deficiencies, weaknesses, and areas of non-compliance as soon as may be practicable considering Cisco's prioritization of such, based upon their criticality (e.g. nature, severity, likelihood).

d. **Status of Remedial Action.** Upon request, Cisco shall keep Customer reasonably informed of the status of any remedial action that is required to be carried out, including the estimated timetable for completing the same.

4.9. Contractor Relationships

a. **Policies.** Cisco shall have information security policies or procedures for its use of external Representatives that impose requirements consistent with this document.

b. **Monitoring.** Cisco shall monitor and audit service delivery by its external Representatives and review its external Representatives' security practices against the security requirements set forth in Cisco's agreements with such Representatives.

4.10. Management of Data Breaches and Improvements

a. **Responsibilities and Procedures.** Cisco shall establish procedures to ensure a quick, effective, and orderly response to Data Breaches.

b. **Reporting Data Breaches.** Cisco shall implement procedures for Data Breaches to be reported as appropriate. Representatives should be made aware of their responsibility to report Data Breaches as quickly as reasonably possible.

c. **Reporting Information Security Weaknesses.** Cisco's Representatives are required to note and report any observed or suspected information security weaknesses in systems or services.

d. **Assessment of Information Security Events.** Cisco shall have classification scale in place in order to decide whether an information security event should be classified as a Data Breach.

e. **Response Process.** Cisco shall maintain a record of Data Breaches with a description of the incident, the effect of the incident, the name of the reporter and to whom the incident was reported, the procedure for rectifying the incident, and the remedial action taken to prevent future security incidents.

4.11. Information Security Aspects of Business Continuity Management

a. **Planning.** Cisco shall maintain emergency and contingency plans for the facilities where Cisco information systems that process Data are located. Cisco shall verify the established and implemented information security continuity controls at regular intervals.

b. **Data Recovery.** Where and as applicable, Cisco shall design redundant storage and procedures for recovering Data in its possession or control in a manner sufficient to reconstruct Data in its original state as found on the last recorded backup provided by the Customer or in a manner sufficient to resume the Service.

5. Definitions

5.1. **"Affiliates"** means companies within the Cisco group that may process Data in order to provide the Products and/or Services. Such Affiliates include Cisco Systems, Inc., Cisco Commerce India Private Limited, Cisco Systems G.K., Cisco Systems Australia Pty Limited, Cisco Systems Canada Co., Cisco International Limited, Cisco Systems (Italy) S.R.L., Cisco Systems International
B.V., ThousandEyes LLC, Broadsoft, Inc., AppDynamics LLC, AppDynamics International Ltd. and Meraki LLC. Unless otherwise explicitly agreed by the Parties, any legal entities which become part of the Cisco group of companies through an acquisition or merger are not considered Affiliates for the purposes of this document.

5.2. **"Agreement"** means the written or electronic agreement between Customer and Cisco or the relevant Cisco Affiliate for the provision of the Services and/or Products to Customer.

5.3. **"Customer Content"** means data such as text, audio, video or image files, provided by you to Cisco in connection with your use of Cisco solutions, and data developed at your specific request related to a statement of work or contract.

5.4. **"Data Breach"** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Data relating to you.

5.5. **"Personal Data"** means any information about, or relating to, an identifiable individual. It includes any information that can be linked to an individual or used to directly or indirectly identify an individual, natural person.

5.6. **"Product"** means Cisco or its Affiliates' branded hardware and software that is purchased under the Agreement.

5.7. **"Representatives"** means Cisco's or its Affiliates' officers, directors, employees, agents, contractors, temporary personnel, subcontractors and consultants.

5.8. **"Service"** means Cisco or its Affiliates' branded service offering that is purchased by Customer under the Agreement.

5.9. **"Sensitive Personal Data"** refers to sensitive personal information (as defined under the California Consumer Protection Act), special categories of personal data (as described in Article 9 of the General Data Protection Regulation), and other similar categories of Personal Data that are afforded a higher level of protection under applicable law.

5.10. **"Systems Information"** means data generated or collected in connection with your use and operation of Cisco solutions, and data provided by you in connection with our delivery of products and services to you (including, for example, when you submit a request related to support services). Systems Information is

composed of Telemetry Data, Support Data, Install Base Information, Entitlement Information, Customer Feedback and Security Threat Data as defined further here.

The data importer informs the data exporter of any update of the security measures detailed in this Exhibit C. Any such update fully complies with the requirements laid down in this Agreement as well as with Regulation (EU) 2018/1725 and, in particular, its Chapter V and the *Ad Hoc* Contractual Clauses in Exhibit A.

EXHIBIT D

ATTACHMENT 1 - WEBEX MEETINGS PRIVACY DATA SHEET

This Privacy Data Sheet describes the processing of personal data (or personally identifiable information) by Cisco Webex Meetings.

Cisco Webex Meetings is a cloud-based web and video conferencing solution made available by Cisco to companies or persons who acquire it for use by their authorized users.

Cisco will process personal data from Cisco Webex Meetings in a manner that is consistent with this Privacy Data Sheet. In jurisdictions that distinguish between Data Controllers and Data Processors, Cisco is the Data Controller for the personal data processed to administer and manage the customer relationship. Cisco is the Data Processor for the personal data processed by Cisco Webex Meetings in order to provide its functionality.

Note: This Privacy Data Sheet is a supplement to the Cisco Online Privacy Statement.

1. Overview

Cisco Webex Meetings (the "Service" or "Webex Meetings") is a cloud-based web and video conferencing solution made available by Cisco to companies or persons ("Customers," "you," or "your") who acquire it for use by their authorized users (each, a "user"). The Service enables global employees and virtual teams to collaborate in real time from anywhere, anytime, on mobile devices or video systems as though they were working in the same room. Solutions include meetings, events, training, and support services. For more information regarding optional features for Cisco Webex Meetings, please see the Addendums below.

Because the Service enables collaboration among its users, as described below, your personal data is required in order to use the Service. The following paragraphs describe Cisco's processing of personal data in connection with the delivery of the Service, the location and transfers of that data, and how it is secured in accordance with privacy principles, laws, and regulations. Cisco will use your personal data consistent with this Privacy Data Sheet to serve the legitimate interests and fulfill the contractual obligations of providing the Solution.

This Privacy Data Sheet covers the Cisco Webex Meetings, Cisco Webex Events, Cisco Webex Training, and Cisco Webex Support. If you use the Service together with the Cisco Webex App, see the see the Cisco Webex App Privacy Data Sheet (available on The Cisco Trust Center) for descriptions of the data that may be collected and processed in connection with those services.

For a detailed overview of the Service, please visit the Cisco Web Conferencing homepage.

2. Personal Data Processing

The Service allows users to instantly connect in a way that is almost as personal as a face-to-face meeting. If you are a user and your employer is the Customer that acquired the Service, your employer serves as the "data controller" of data processed by the Service (see the Webex Meetings Privacy Data Map for a visualization of who is doing what with data). The information described in the table below and in this Privacy Data Sheet is accessible to your employer and is subject to your employer's policies regarding access, use, monitoring, deletion, preservation, and export of information associated with the Service.

Similarly, if users participate in meetings hosted by users in other companies, the meeting host will control any meeting recordings or files shared during the meeting, which will be subject to the host's corporate policies regarding access, use, monitoring, deletion, preservation, and export of information. The meeting host has the option to record meetings, which may be shared with others or discoverable in a legal matter. The meeting host should inform all meeting attendees prior to recording and Webex displays a red circle and plays an audio prompt to all participants indicating that the meeting is being recorded. Note, Cisco has no control over, and is not responsible or liable for the privacy of any information that you have shared with others. Even after you remove information from the Webex Meetings platform, copies of that information may remain viewable elsewhere to the extent it has been shared with others.

The table below list the categories of personal data used by the Service and describe why we process such data. Cisco Webex Meetings does not:

ii. Produce decisions that would result in legal or other significant effects impacting the rights of data subjects based solely by automated means.
iii. Sell your personal data.
iv. Serve advertisements on our platform.
v. Track your usage or content for advertising purposes.
vi. Monitor or interfere with you your meeting traffic or content.
vii. Monitor or track user geolocation.

Personal Data Category	Type of Personal Data	Purpose of Processing
User Information	• Name • Email Address • Password • Browser • Phone Number (Optional) • Mailing Address (Optional) • Avatar (Optional) • User Information Included in Your Directory (if synched) • Unique User ID (UUID) (a pseudonymized 128-bit number assigned to compute nodes on a network)	We use User Information to: • Provide you with the Service • Enroll you in the Service • Display your user avatar and profile to other users • Make improvements to the Service and other Cisco products and services • Provide you support • Customer relationship management (e.g., transactional communication) • Authenticate and authorize access to your account • Bill you for the Service • Display directory information to other Webex users (Avatar may be cached locally on devices of other Webex users that attend meetings with you for a period of 2 weeks)

Host and Usage Information	• IP Address
	• User Agent Identifier
	• Hardware Type
	• Operating System Type and Version
	• Client Version
	• IP Addresses Along the Network Path
	• MAC Address of Your Client (As
	• Applicable)
	• Service Version
	• Actions Taken
	• Geographic Region (i.e., Country Code)
	• Meeting Session Information (e.g., date and time, frequency, average and actual duration, quantity, quality, network activity, and network connectivity)
	• Number of Meetings
	• Number of Screen-Sharing and NonScreen-Sharing Sessions
	• Number of Participants
	• Screen Resolution
	• Join Method
	• Performance, Troubleshooting, and Diagnostics Information
	· Meeting Host Information[1]
	  • Host Name and email address
	  • Meeting Site URL
	  • Meeting Start/End Time
	• Meeting Title
	• Call attendee information, including email addresses, IP address,
		We use Host and Usage Information to:
		• Provide you with the Service
		• Understand how the Service is used
		• Diagnose technical issues
		Conduct analytics and statistical analysis in aggregate form to improve the technical performance of the Service
		• Respond to Customer support requests
		• Make improvements to the Service and other Cisco products and services
		
		Cisco may use metadata from Webex meetings (e.g., meeting participants, frequencies) to:
		• help organize, sort, and/or prioritize your Webex App messages or spaces in a way that is relevant to you and your work
		• Provide you the Personal Insights feature (optional)

	username, phone numbers, room device information • Information submitted through attendee registration form (Optional)	
User-Generated Information	• Meeting Recordings (if enabled by Customer) • Transcriptions of meeting recordings (optional, only applicable if enabled by you) • Uploaded Files (for Webex Events and Training only)	We use User-Generated Information to: • Provide you with the Service

[1] Used for billing purpose

Calendar

If you use a Webex plug-in with your Calendar service or utilize Webex Hybrid Calendar Services, we will only use the data set forth above regarding meeting dates, times, title and participants. For more information on Webex Hybrid Calendar Service see the Office 365 and Google Calendar integration references.

Technical Support Assistance

If a Customer reaches out to Cisco Technical Assistance Center (TAC) for problem diagnosis and resolution, Cisco TAC may receive and process personal data from the Service. The Cisco TAC Service Delivery Privacy Data Sheet describes Cisco's processing of such data.

Control Hub

Cisco Webex Control Hub Analytics provides usage trends and valuable insights that can be used to help with strategies to promote and optimize adoption across teams. Cisco Webex Control Hub Analytics uses Host and Usage information to provide advanced analytics capabilities and reports.

Polling

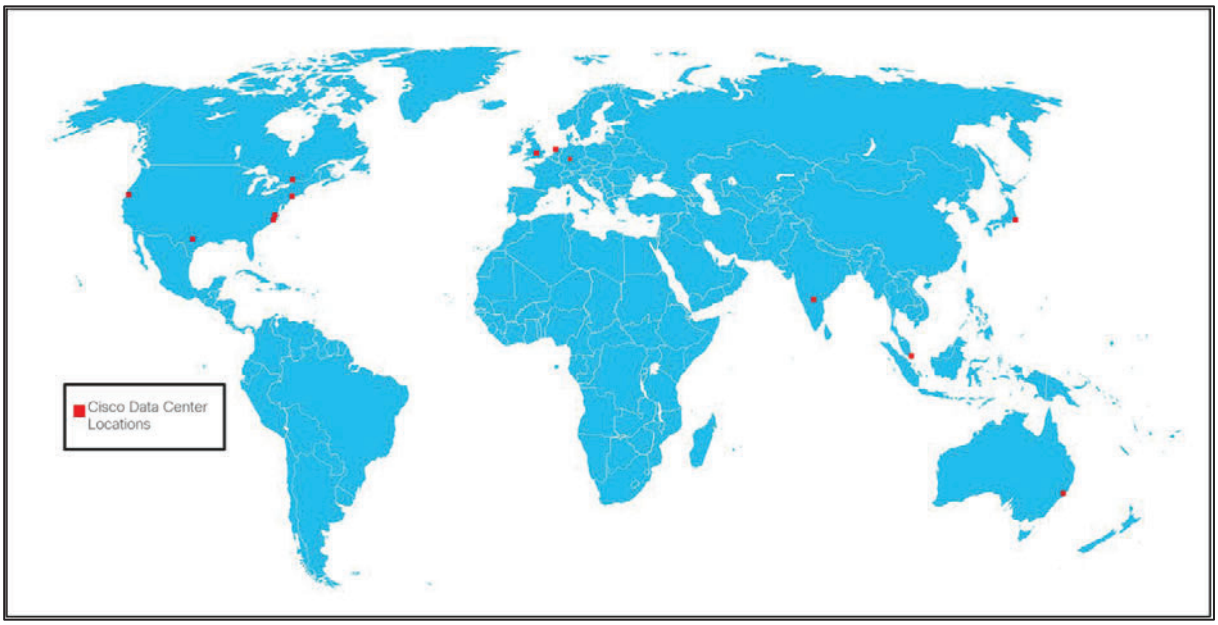
As a presenter, you can use a poll to create and share questionnaires. Any polling data collected from participants will be deleted once the meeting has ended. Some Webex Meetings may feature Slido, which is a cloud-based polling and Q&A solution; for details around the processing of personal data by the Slido feature, please see Addendum 5 to this Privacy Data Sheet.

Extended Security Pack

If you purchase the extended security pack, please see the Cloudlock Privacy Data Sheet for Cloudlock data privacy information.

3. Data Center Locations

The Service leverages its own data centers to deliver the Service globally. If you join a meeting using Cisco Webex App, please see the Cisco Webex App Privacy Data Sheet for applicable privacy information, including data center locations. The Webex Meetings data centers are currently located in the following countries (data center locations may change from time to time and this Privacy Data Sheet will be updated to reflect those changes):



User-Generated Information is stored in the data center in Customer's region as provided during the ordering process. Data is replicated across data centers within the same region to ensure availability.

Cisco Data Center Locations	Internet Point of Presence (iPOP) Locations
Amsterdam, Netherlands	Amsterdam, Netherlands
Bangalore, India	California, USA
California, USA	Illinois, USA
Frankfurt, Germany	New Jersey, USA
London, UK	Sydney, Australia
Montreal, Canada	Texas, USA
New York, USA	
North Carolina, USA	
Singapore, Singapore	
Sydney, Australia	
Texas, USA	
Tokyo, Japan	
Toronto, Canada	
Virginia, USA	

An Internet Point of Presence (iPOP) Location is used to route traffic geographically from nearby areas to a Cisco Data Center Location. It is intended to route Webex Meeting traffic through Cisco's infrastructure and improve performance. Data routed through iPOP Locations remains encrypted and is not stored in that location.

For free user accounts, the data defined in this privacy data sheet may be stored in a Webex data center outside the account holder's region.

4. Webex Data Residency

Webex data residency provides Customer user administrators the ability to choose where their organization's data is stored. Data residency is currently available for Customers in the European Union (EU) ("EU Customers") for personal data processed by Webex Meetings, including User Information, Host & Usage Information, and User-Generated Information (other than as noted below). For those EU Customers that became Webex Meetings Customers after July 2021, data is by default stored where those Customers are provisioned. For EU Customers who were provisioned before July 2021, user administrators will be provided instructions on how to migrate their user data, through Control Hub, to the location where they are provisioned.

To facilitate certain operations and aspects of the Service, certain exceptions to Webex data residency exist; specifically, cross-border transfers of personal data may still occur when (a) a user registers on any Cisco platform (for example, through www.webex.com or www.cisco.com) or through any Cisco service to learn more about Cisco products or events; (b) a Customer provides ordering information (business contact information); (c) a user engages in collaboration with users outside of the EU region; (d) a user requests technical support through Cisco's Technical Assistance Center ("TAC") (in which case the information that a user provides within the initial TAC request may be transferred outside region); (e) a user enables certain optional functionalities; or (f) a user enables cell phone "push" notifications (in which case the cell phone provider associated with iOS or Android functionality may transfer data outside of the region). Additionally, until August 2022, some Host and Usage information will continue to incur cross-border transfers outside of the region, for billing purposes.

For free user accounts, the data defined in this privacy data sheet may be stored in a Webex data center outside the account holder's region, including for EU Customers.

5. Cross-Border Data Transfer Mechanisms

Cisco has invested in transfer mechanisms to enable the lawful use of data across jurisdictions:

i. Binding Corporate Rules (Controller)
ii. APEC Cross-Border Privacy Rules
iii. APEC Privacy Recognition for Processors
iv. EU Standard Contractual Clauses

6. Access Control

The table below lists the personal data used by Cisco Webex Meetings to carry out the Service, who can access that data, and why.

Personal Data Category	Who has Access	Purpose of the Access
User Information	User through the My Webex Page	Modify, control, and delete User Information

	Customer through the Site Admin Page or Webex Control Hub	Modify, control, and delete in accordance with Customer's personal data policy
	Cisco	Support the Service in accordance with Cisco's data access and security controls process
Host and Usage Information	Host through the My Webex Page	View meeting session Information
	Customer may view this information through the Site Admin Page, Webex Control Hub, or may be otherwise provided by Cisco	View usage, meeting session and configuration information
	Cisco	Support and improvement of the Service by the Cisco Webex Meetings support and development team
User Generated Information	User through the My Webex Page	Modify, control, and delete based on user's preference
	Customer using APIs provided with the Service or through the Site Admin Page or Webex Control Hub	Modify, control, and delete in accordance with Customer's personal data policy
	Cisco	While Cisco operates the Service, Cisco will not access this data unless it is shared with Cisco by Customer, and will only access it in accordance with Cisco's data access and security controls process.
	Other Customers and users (when shared during a meeting)	Content you choose to share during a meeting may be accessed by users in the meeting, wherever they are located. Even after you remove information from the Service, copies of that content may remain viewable elsewhere to the extent it has been shared with others.

7. Data Portability

The Service allows Customers and users to export all User-Generated Information. A Customer's administrator may do so using APIs provided with the Service (recordings only) or through the Site Admin Page; while individual users may do so through the My Webex Page. Meeting recordings are available in standard mp4 format .

Customers are permitted to export personal data collected about their users on the Webex Meetings platform using APIs or via the Site Admin Configuration.

8. Data Deletion and Retention

Subject to their employer's corporate retention policies, users with an active subscription can delete User-Generated Information from their account through the My Webex Page at any time during the term of their subscription. Enterprise Customers have the ability to set organization-wide retention periods for recordings using APIs. Cisco provides free account users up to 6 months of free storage.

The table below lists the personal data used by Cisco Webex Meetings, the length of time that data needs to be retained, and why we retain it.

Users seeking deletion of User Information and User Generated Information retained on their employer's Webex Meetings site must request deletion from their employer's site administrator.

Type of Personal Data	Retention Period	Reason for Retention
User Information	Active Subscriptions: • User Information will be maintained as long as Customer maintains active subscription (paid or free). Terminated Service: • Deleted once the Service is terminated • Name and UUID are maintained 7 years from termination	Name and UUID are maintained 7 years from termination as part of Cisco's business records and are maintained to comply with Cisco's financial and audit requirements. Any billing information is also subject to this retention period.
Host and Usage Information	3 years	Host and Usage information is kept as part of Cisco's record of Service delivery. * Any billing information is retained for 7 years as part of Cisco's business records and are maintained to comply with Cisco's financial and audit requirements. Once the specified retention period has expired, data will be deleted.
User Generated Information	Active Subscriptions: • At Customer's or user's discretion Terminated Service: Deleted within 60 days	User-Generated Information, except for recordings, is not retained on the Webex Meetings platform when Customer or user deletes this data. Recordings are "soft deleted" and retained for 30 days before being removed from the platform, to allow a Customer or user to retrieve a recording they have inadvertently deleted. User Generated Information is retained for 60 days after services are terminated to give Customers opportunity to download.

9. Personal Data Security

The Service adopts technical and organizational security measures designed to protect your personal data from unauthorized access use or disclosure. Additional information about our encryption architecture is summarized in the table and paragraphs below.

Personal Data Category	Security Controls and Measures
User Information	Encrypted in transit and at rest
Passwords (stored if Single Sign On is not configured)	Encrypted and hashed in transit and at rest
Host and Usage Information	Encrypted in transit and at rest
User Generated Information	Recordings prior to May 2018 were encrypted in transit with the option to encrypt at rest. Recordings created after May 2018 are encrypted in transit and at rest by default. Recordings created in the Webex Meetings FedRAMP-Authorized service after October 2019 are encrypted in transit and at rest.
User Information	Encrypted in transit and at rest

Protecting Data at Rest

The Service encrypts User Information, Passwords and User Generated Information, as described above, at rest.

Encryption of Data in Transit

All communications between cloud registered Webex Apps, Webex Room devices and Webex services occur over encrypted channels. Webex uses the TLS protocol with version 1.2 or later with high strength cipher suites for signalling.

After a session is established over TLS, all media streams (audio VoIP, video, screen share, and document share) are encrypted.

Encrypted media can be transported over UDP, TCP, or TLS. Cisco prefers and strongly recommends UDP as the transport protocol for Webex voice and video media streams. This is because TCP and TLS are connection orientated transport protocols, designed to reliably deliver correctly ordered data to upper-layer protocols. Using TCP or TLS, the sender will retransmit lost packets until they are acknowledged, and the receiver will buffer the packet stream until the lost packets are recovered. For media streams over TCP or TLS, this behaviour manifests itself as increased latency/jitter, which in turn affects the media quality experienced by the call's participants.

Media packets are encrypted using either AES 256 or AES 128 based ciphers. The Webex App and Webex Room devices uses AES-256-GCM to encrypt media; these media encryption keys are exchanged over TLS-secured signalling channels. SIP and H323 devices that support media encryption with SRTP can use AES-256-GCM, AES-128-GCM, or AES-CM-128-HMAC-SHA1 (AES-256-GCM is the Webex preferred media encryption cipher).

Zero Trust Security Based End-to-End Encryption

For standard Webex Meetings, where devices and services use SRTP to encrypt media on a hop by hop basis, Webex media servers need access to the media encryption keys to decrypt the media for each SRTP call leg. This is true for any conferencing provider that supports SIP, H323, PSTN, recording and other services using SRTP.

However, for businesses requiring a higher level of security, Webex also provides end-to-end encryption for meetings ("Webex Zero Trust Security end-to-end encryption"). With this option, the Webex cloud does not have access to the encryption keys used by meeting participants and cannot decrypt their media streams. Webex Zero Trust Security end-to-end encryption uses standard track protocols to generate a shared meeting encryption key (Messaging Layer Security (MLS)) and to encrypt meeting content (Secure Frame (S-Frame). With MLS, the meeting encryption key is generated by each participant's device using a combination of the shared public key of every participant and the participant's private key (never shared). The meeting encryption key does not traverse the cloud and is rotated as participants join and leave the meeting. For more details on Zero Trust Security based end-to-end encryption see the Zero Trust Security for Webex white paper.

With end-to-end encryption, all meeting content (voice, video, chat, etc.) is encrypted using the locally derived meeting encryption key. This data cannot be deciphered by the Service.

Note that when end-to-end encryption is enabled, Webex services and endpoints that need access to meeting keys to decrypt content (e.g. devices using SRTP where encryption is performed hop by hop) are not supported. This restricts meeting participants to those using the Webex App or cloud registered Webex devices only, and excludes services such as network-based recording, speech recognition etc. The following features are also not supported:

- Join Before Host
- Video-device enabled meetings
- Lnux clients
- Network-Based Recording (NBR)
- Webex Assistant
- Saving session data transcripts, Meeting Notes
- PSTN Call-in/Call-back

10. Sub-processors

We may share data with service providers, contractors or authorized third parties to assist in providing and improving the Service. We do not rent or sell your information. All sharing of information is carried out consistent with the Cisco Privacy Statement and we contract with third-party service providers that can provide the same level of data protection and information security that you can expect from Cisco. Below is a list of sub-processors for Webex Meetings. Data shared with these sub-processors follows Webex data residency, except for those sub-processors who may be implicated by one of the exceptions listed in that section.

All Cisco sub-processors undergo a rigorous security and privacy assessment to confirm their compliance with our requirements. They are further bound by a data processing agreement which incorporates the EU Standard Contractual Clauses and places strict limits on their use and processing of any data provided by us or our Webex customers and users.

Sub-processor	Personal Data	Service Type	Location of Data Center

Akamai	IP address, Browser and Geographic region	Akamai is used as content delivery network (CDN) services provider for static content. Akamai does not store content but may store IP address in logs for a maximum of 3 years.	Location generally maps to Customer's Webex data center assignment. To the extent Akamai receives IP addresses of Webex Meeting customers, those IP addresses may be transmitted to the United States with strict access control means and appropriate safeguards under the EU Standard Contractual Clauses (SCCs).
Amazon Web Services (AWS)	Limited Host & Usage Information and Meeting Recording File (if applicable)	AWS cloud infrastructure is used to host the Webex signaling service that processes meeting participant UUIDs, meetings start and end times. Data will be deleted within 15 days of the meeting. (Location maps to Customer's Webex data center assignment.) AWS cloud infrastructure is used to host Webex media nodes that may process real-time meeting data such as VoIP, video and high frame rate sharing data. This information is not retained in AWS once your meeting has ended. AWS cloud infrastructure is also used to store meeting recording files, if meeting record is enabled by the Customer. (Location maps to Customer's Webex data center assignment).	United States Germany Netherlands United Kingdom Brazil Australia Japan Singapore
WalkMe[2]	Unique User ID (UUID) and user region	Provides user with a step-by-step tour and guidance on how to use Webex Meetings online site.	Globally
Vbrick	Name, UUID, email address	Vbrick provides users with extended capacity for Webex Meetings including over 3,000 participants. Vbrick requires the data for authentication and the data is encrypted in transit. Vbrick does not store Webex Customer personal data.	United States EU: Germany, Ireland Australia

[2] Customers may turn this feature off at any time. Feature is currently enabled for non-enterprise Webex sites.

If a Customer acquires the Service through a Cisco partner, we may share any or all of the information described in this Data Sheet with the partner. Customers have the option of disabling this information-sharing with Cisco partners. If you use a third-party account to sign-in to your Webex account, Cisco may share only the necessary information with such third party for authentication purposes.

11. Information Security Incident Management

Breach and Incident Notification Processes

The Information Security team within Cisco's Security & Trust Organization coordinates the Data Incident Response Process and manages the enterprise-wide response to data-centric incidents. The Incident Commander directs and coordinates Cisco's response, leveraging diverse teams including the Cisco Product Security Incident Response Team (PSIRT), the Cisco Security Incident Response Team (CSIRT), and the Advanced Security Initiatives Group (ASIG).

PSIRT manages the receipt, investigation, and public reporting of security vulnerabilities related to Cisco products and networks. The team works with Customers, independent security researchers, consultants, industry organizations, and other vendors to identify possible security issues with Cisco products and networks. The Cisco Security Center details the process for reporting security incidents.

The Cisco Notification Service allows Customers to subscribe and receive important Cisco product and technology information, including Cisco security advisories for critical and high severity security vulnerabilities. This service allows Customers to choose the timing of notifications, and the notification delivery method (email message or RSS feed). The level of access is determined by the subscriber's relationship with Cisco. If you have questions or concerns about any product or security notifications, contact your Cisco sales representative.

12. Certifications and Compliance with Privacy Requirements

The Security & Trust Organization and Cisco Legal provide risk and compliance management and consultation services to help drive security and regulatory compliance into the design of Cisco products and services. The Service is built with privacy in mind and is designed so that it can be used in a manner consistent with global privacy requirements., , including the EU General Data Protection Regulation, California Consumer Privacy Act, Canada's Personal Information Protection and Electronic Documents Act and Personal Health Information Protection Act.

In addition to the Cross-Border Data Transfer Mechanisms/Certifications listed in Section 4, Cisco has the following:

i. EU-US Privacy Shield Framework
ii. Swiss-US Privacy Shield Framework

Further, In addition to complying with our stringent internal standards, Cisco also continually maintains third-party validations to demonstrate our commitment to information security. The Service has received the following certifications:

i. EU Cloud Code of Conduct Adherence by SCOPE Europe
ii. ISO 27001, 27017, 27018, 27701
iii. SOC 2 Type II Attestation, SOC 3, + C5
iv. CSA STAR 2
v. FedRAMP
vi. Esquema Nacional de Seguridad (ENS) (Spain)
vii. Information System Security Management and Assessment Program (Japan)

13. Exercising Data Subject Rights

Users whose personal data is processed by the Service have the right to request access, rectification, suspension of processing, or deletion of the personal data processed by the Service.

We will confirm identification (typically with the email address associated with a Cisco account) before responding to the request. If we cannot comply with the request, we will provide an explanation. Please note, users whose employer is the Customer/Controller, may be redirect to their employer for a response.

Requests can be made by submitting a request via:

1) the Cisco Privacy Request form
2) by postal mail:

<table>
<tr><td colspan="3">Chief Privacy Officer Cisco
Systems, Inc. 170 W. Tasman
Drive San Jose, CA 95134
UNITED STATES</td></tr>
<tr><td>Americas Privacy
Officer
Cisco Systems, Inc.
170 W. Tasman Drive

San Jose, CA 95134
UNITED STATES</td><td>APJC Privacy Officer

Cisco Systems (USA) Pte Ltd
Bldg 80, Lvl 25, Mapletree Biz
City,
80 Pasir Panjang Road,
Singapore, 117372
SINGAPORE</td><td>EMEAR Privacy Officer

Cisco Systems, Inc.
Haarlerbergweg 13-19, 1101 CH

Amsterdam-Zuidoost NETHERLANDS</td></tr>
</table>

We will endeavor to timely and satisfactorily respond to inquiries and requests. If a privacy concern related to the personal data processed or transferred by Cisco remains unresolved, contact Cisco's US-based third-party dispute resolution provider.

Alternatively, you can contact the data protection supervisory authority in your jurisdiction for assistance. Cisco's main establishment in the EU is in the Netherlands. As such, our EU lead authority is the Dutch Autoritiet Persoonsgegevens.

14. General Information

For more general information and FAQs related to Cisco's Security and Privacy Program please visit The Cisco Trust Center.

Cisco Privacy Data Sheets are reviewed and updated on an annual, or as needed, basis. For the most current version, go to the Personal Data Privacy section of the Cisco Trust Center.

Addendum One: People Insights for Cisco Webex

This Addendum describes the processing of personal data (or personal identifiable information) by People Insights for Cisco Webex Meetings and Cisco Webex.

People Insights for Cisco Webex Meetings and Cisco Webex is a cloud-based company directory solution made available by Cisco to companies or persons who acquire it for use by their authorized users.

Cisco will process personal data from People Insights for Cisco Webex Meetings and Cisco Webex in a manner that is consistent with this Privacy Data Sheet. In jurisdictions that distinguish between Data Controllers and Data Processors, Cisco is the Data Controller for the personal data processed to administer and manage the Customer relationship. Cisco is the Data Processor for the personal data processed by Cisco Webex Meetings in order to provide its functionality.

Note: This Privacy Data Sheet is a supplement to the Cisco Online Privacy Statement.

1. Overview

The People Insights feature ("People Insights" or the "Feature") provides Cisco Webex users with comprehensive, publicly available business and professional information for meeting participants giving users context and increased insight about the people with whom they collaborate. People Insights only displays publicly available information, similar to what can be found in search engine results for a person's name and profession. People Insights will also display internal company directory information to users in the same company. This internal directory information is not visible to users outside the company. The People Insights database doesn't look behind logins or paywalls, which means your profile won't be populated with content from sites like Facebook.

People Insights was designed with data protection and privacy in mind, and is aligned to global privacy requirements, including GDPR. This feature provides users with a convenient single view into their already existing public presence and digital footprint. As outlined below, People Insights includes functionality to honor data subject rights. Users fully own their People Insights profile and can change or hide the profile to keep information private.

People Insights is enabled by default for U.S. provisioned Customers. Customers provisioned in the EU must opt-in to this feature. Users at an enabled organization can opt-out of People Insights by suppressing their profile from other meeting participants' view. This is accomplished in two ways:

1. Entering a meeting and selecting the "Hide Profile" link,
2. Signing into people.webex.com and clicking on "Hide Profile"

If you join a meeting, or a teamspace, hosted by a Cisco Customer that has People Insights enabled on their site, all participants' People Insight profiles will be visible unless they have chosen to hide their profiles as described above.

2. Personal Data Processing

People Insights compiles business and professional profiles for meeting participants using publicly available and legitimately sourced information, published authored works, news articles, search engine results, via APIs and through content supplied by the profile owner.

The table below lists the personal data processed by People Insights to provide its services and describes why the data is processed.

Personal Data Category	Type of Personal Data	Purpose of Processing
Publicly Available Business and Professional Biographical Data	• Profile Photos • News • Tweets • Authored Works • Bios • Employment History • Education History • Web Links for a specific person	• To source the People Insights profile and to enable search within the feature.
Account & Usage Information	User Level Account Details (including email, name, and web interactions and platform usage)	• To provide support and improvement of the Feature • Product analytics (e.g. frequency of profile edits, # of successful profile loads in a meeting, etc.)

Directory Data	• If the directory option is enabled by the site administrator, professional information including the following may be collected from the internal company directory (as selected by the administrator):
	  • Title
	  • Phone Number
	  • Location
	  • Organization
	  • Department
	  • Photo
	  • Role
	  • Reporting Structure
		• To augment the user's People Insights profile by providing company specific context to meeting participants who belong to the same organization. This data will only be visible to participants within the user's organization.

User Generated Information	• Information that the user adds in their People Insights profile.	• Augment the user's own People Insights profile (visible to Insights users)

3. Data Center Locations

People Insights data is stored on third party servers provided by Amazon Web Services ("AWS"). AWS servers are located in the United States.

4. Cross-Border Data Transfer Mechanisms

Cisco has invested in transfer mechanisms to enable the lawful use of data across jurisdictions:

- Binding Corporate Rules (Controller)
- APEC Cross-Border Privacy Rules
- APEC Privacy Recognition for Processors
- EU Standard Contractual Clauses

5. Access Control

The table below lists the personal data used by People Insights, who can access that data, and why.

Personal Data Category	Who has access	Purpose of the access
Publicly Available Business and Professional Biographical Data	Cisco Users of Customer Webex site with enabled People Insights	To provide the Feature
Account & Usage Information	Cisco	Registration Support Correlate users with correct profiles Analytics to improve service
	Customer	Feature enablement/disablement.
Directory Data	Customer (Admin) People Insight users within the Customer's organization	Directory data is provided and maintained by Customer administrator to allow integration into People Insights profile.
	Cisco	Directory data is imported and integrated with Customer profile data to support profile development
User-Generated Information	User	Users may access their own User-Generated Information to edit or delete content.

6. Data Portability

Individuals can receive a copy of their own People Insights profile, including their self-generated information, through the Cisco Privacy Request form

7. Data Deletion and Retention

The table below lists the personal data used by People Insights, the length of time that data needs to be retained, and why we retain it.

Type of Personal Data	Retention Period	Reason for Retention
Publicly Available Business & Professional Data	Obtained from public websites: Indefinite Obtained through third-party APIs: In accordance with contractual requirements	Publicly Available Business & Professional Data is derived from public sources. It is retained indefinitely by default. Upon request, publication and links to source data can be suppressed and restricted from view and publication. As publicly available data originates from outside of Cisco WebEx, any permanent changes or deletions must be addressed and requested with the primary source. At the request of users, the data can be archived in order to not appear. This allows for the data to remain permanently hidden rather than re- appearing with a new search after being previously purged.
Account & Usage Information	Active Subscriptions: At Customer's or user's discretion Deactivated Accounts: Deleted within thirty (30) days	Users can request to remove their Account Information by opening a TAC service request. Cisco will respond to such requests within 30 days.
Directory Data	Active Subscriptions: At Customer's or user's discretion Deactivated Accounts: Deleted within thirty (30) days	Administrators can disable Active Directory feature while still enabling People Insights. Directory data will be hard deleted in this case of deactivation. Non-directory data will remain, with the exception of name and email for users who had only directory data in their profile before the deactivation.
User-Generated Information	Active Subscriptions: At Customer's or user's discretion Deactivated Accounts: Deleted within thirty (30) days	Users can delete User-Generated Information from their profile at any time.

8. Personal Data Security

Cisco has implemented appropriate technical and organizational measures designed to secure personal data from accidental loss and unauthorized access, use, alteration, and disclosure.

Personal Data Category	Security controls and measures
Publicly Available Business & Professional Data	**Encrypted in transit, AES 256 for storage, Keys managed through AWS KMS**
Host & Usage Information	**Encrypted in transit, AES 256 for storage, Keys managed through AWS KMS**
Directory Data	**Encrypted in transit, AES 256 for storage, Keys managed through AWS KMS**
User-Generated Information	**Encrypted in transit, AES 256 for storage, Keys managed through AWS KMS**

9. Sub-processors

Cisco partners with service providers that act as sub-processors and contract to provide the same level of data protection and information security that you can expect from Cisco. A current list of sub-processors for the Feature is below:

Sub-processor	Personal Data	Service Type	Location of Data Center
Amazon Web Services	• Publicly Available Business & Professional Data • Host & Usage Information • Directory Data • User-Generated Information	Cloud Storage	United States
Amplitude	• Host & Usage Information	User Analytics	United States
Diffbot	• Name, Email	Supplementing Publicly Available Business & Professional Data	United States

10. Sub-processors

Cisco partners with service providers that act as sub-processors and contract to provide the same level of data protection and information security that you can expect from Cisco. A current list of sub-processors for the Feature is below:

Sub-processor	Personal Data	Service Type	Location of Data Center
Amazon Web Services	• Publicly Available Business & Professional Data • Host & Usage Information • Directory Data • User-Generated Information	Cloud Storage	United States
Amplitude	• Host & Usage Information	User Analytics	United States
Diffbot	• Name, Email	Supplementing Publicly Available Business & Professional Data	United States

Addendum Two: Facial Recognition for Cisco Webex Meetings (Optional)

This Addendum describes the processing of personal data (or personal identifiable information) by Facial Recognition feature for Cisco Webex Meetings. The Facial Recognition feature is only available when using Webex Meetings on certain Cisco Endpoint devices.

Facial Recognition feature for Cisco Webex Meetings is a cloud-based feature solution made available by Cisco to companies or persons who acquire it for use by their authorized users.

Cisco will process personal data from Facial Recognition feature for Cisco Webex Meetings in a manner that is consistent with this Privacy Data Sheet. In jurisdictions that distinguish between Data Controllers and Data Processors, Cisco is the Data Controller for the personal data processed to administer and manage the Customer relationship. Cisco is the Data Processor for the personal data processed by Cisco Webex Meetings in order to provide its functionality.

Note: This Privacy Data Sheet is a supplement to the Cisco Online Privacy Statement.

1. Overview

Cisco introduced the facial recognition feature ("Facial Recognition" or the "Feature") to provide Webex Meetings users with the ability to identify and recognize registered Webex meeting participants (i.e., associate participant names with their positions in a Webex meeting video), giving users increased connection to meeting participants. The Feature recognizes a face by converting it to an abstracted facial vector. A facial vector is a list of numbers that characterize salient facial features of a user that is then used to identify who is in the meeting. This level of abstraction allows the system to recognize the same face even when things like lighting and position change.

Facial Recognition is disabled by default, and requires affirmative action by both the Customer and the user to enable. First, the administrator for the Customer may enable Facial Recognition using Webex Control Hub. However, the feature will not be available on the user's account until the user opt-ins at https://settings.webex.com. Because the Feature is based on facial vectors derived from profile images, the user must have a picture taken at the time of enablement.

2. Personal Data Processing

If the user opts-in to the Facial Recognition feature, the Service uses the camera of the user's device to take a profile picture. This picture is sent to the Webex cloud where the Feature algorithm generates a facial vector from the picture so that it can be used for matching as further described below. Both the picture and the facial vector are encrypted and stored securely. The picture may be used to generate a new facial vector in the event Cisco updates or modifies the algorithm by which facial vectors are generated. In the event a Customer or user reaches out to Cisco for support with the Feature, Cisco may also use the picture during the troubleshooting process. During each meeting, a second facial vector is generated, then matched in the Webex cloud against the stored facial vector. This second facial vector is not retained.

The table below lists the personal data processed by Facial Recognition feature to provide its services and describes why the data is processed.

Personal Data Category	Type of Personal Data	Purpose of Processing
User Information	• Name (First, Last) • Email • User ID	• To display name of recognized user • Enroll you in the Feature and enable opt-in
Biometrics	• User facial image • Facial vector mapping	• To create facial vector mapping and provide the facial recognition feature • To generate a new facial vector in case of a modification or update to the Feature algorithm

Host & Usage Information	• Information regarding accuracy of product, including:
	  ○ Successful and unsuccessful facial vector matching
	  ○ User feedback
		• To provide support and product analytics

Location	• Meeting Room Proximity data	• Proximity data is used to improve Facial Recognition to assure facial vectors are matched to the correct users in the correct locations
Calendar	• Meeting Room Calendar Information	• Calendar information is used to improve Facial Recognition to assure facial vectors are matched to the correct users in the correct locations

3. Cross-Border Data Transfer Mechanisms

Cisco has invested in transfer mechanisms to enable the lawful use of data across jurisdictions:

- Binding Corporate Rules (Controller)
- APEC Cross-Border Privacy Rules
- APEC Privacy Recognition for Processors
- EU Standard Contractual Clauses

4. Access Control

The table below lists the personal data used by Facial Recognition feature to carry out the service, who can access that data, and why.

Personal Data Category	Who has access	Purpose of the access
User Information	Cisco	• To display name of recognized user • Enroll you in the Feature and enable opt-in
	Customer	• View user facial recognition registration status
	Users through https://settings.webex.com/	• View and modify facial recognition registration details
Biometrics	Cisco	• To provide the Facial Recognition feature • Algorithm improvement • To troubleshoot issues in the event Customer or users request support

Host & Usage Information	Cisco	• To provide support and product analytics
Location	Cisco	• Proximity data is used to improve Facial Recognition to assure facial vectors are matched to the correct users in the correct locations
Calendar	Cisco	• Calendar information is used to improve Facial Recognition to assure facial vectors are matched to the correct users in the correct locations

5. Data Portability

While Webex Meetings allows Customers and users to export data as described in Section 5 of the Webex Meetings Data Privacy Sheet, it does not support the automatic export of Facial Recognition data.

6. Data Deletion and Retention

The table below lists the personal data used by Facial Recognition feature, the length of time that data needs to be retained, and why we retain it.

Type of Personal Data	Retention Period	Reason for Retention
User Information	User ID is maintained for all active Webex Meetings users. Once a user is deleted from a Customer's account, the User ID is also deleted from the Facial Recognition feature. All other User Information is not stored or retained by the Facial Recognition feature as this information is already stored by Webex Meetings.	User ID is used to track your enrollment in the Feature Names are displayed upon a match in the facial recognition feature.
Biometrics	Images: Users control their image retention. The image is retained as long as the feature is enabled and the user leaves the image associated with their profile. The image can be deleted at any time by user. Images for all users are deleted upon Customer's discontinuation of the Service.	The image is used to provide the Facial Recognition feature, update the facial vector in case of an update to the algorithm, and to troubleshoot issues when requested by a Customer or user.
	Facial vectors are retained as long as the facial images, but are stored separately. Facial vectors are deleted upon discontinuation of the Service.	The facial vectors are used to provide the facial recognition feature.

Host & Usage Information	2 weeks	To provide support and product analytics
Location	2 days	Proximity data is used to improve facial recognition to assure images are assigned to the correct users in the correct locations.
Calendar	Facial Recognition does not store or retain this information separately than already maintained by Webex Meetings.	

7. Personal Data Security

Cisco has implemented appropriate technical and organizational measures designed to secure personal data from accidental loss and unauthorized access, use, alteration, and disclosure.

The table below summarizes encryption architecture of data stored specifically for the Facial Recognition feature.

Personal Data Category	Security controls and measures
User Information	Encrypted in transit, AES 256 for storage
Images	Encrypted in transit, AES 256 for storage
Biometrics	Encrypted in transit, AES 256 for storage
Host & Usage Information	Encrypted in transit, AES 256 for storage
Location	Encrypted in transit, AES 256 for storage

Addendum Three: Webex Closed Captioning (Optional)

This Addendum describes the processing of personal data (or personal identifiable information) by the Closed Captioning feature for Cisco Webex Meetings.

Cisco will process personal data from Closed Captioning in a manner that is consistent with this Privacy Data Sheet. In jurisdictions that distinguish between Data Controllers and Data Processors, Cisco is the Data Controller for the personal data processed to administer and manage the Customer relationship. Cisco is the Data Processor for the personal data processed by Cisco Webex Meetings in order to provide its functionality.

Note: This Privacy Data Sheet is a supplement to the Cisco Online Privacy Statement.

1. Overview

To make your meetings and webinars more accessible, Webex provides automated closed captions which you can turn on without needing to turn on Webex Assistant for Meetings. As people speak, the captions will appear above the meeting or webinar controls. A captions panel is also available, which shows users the captions from the moment they joined the meeting, so they can easily catch up if they miss anything that's being said.

Closed Captioning is a cloud-based feature that is enabled "ON" by default; user administrators can select enablement for specific users or, if a user administrator intends to disable for all users, he or she can request that Cisco disable at an organization level. Users can also disable Closed Captioning, so that captions do not appear for themselves; however, if other users in their meeting(s) have Closed Captioning ON, data belonging to users who have disabled the functionality will still be processed in accordance with the privacy disclosures below.

If a host turns on Webex Assistant for Meetings in addition to Closed Captioning, then they will have additional capabilities to make voice commands and highlight captions to capture audio snippet notes, as detailed in Addendum 4. Additionally, hosts can record the meeting and receive a post-meeting transcript, which they can choose to share with other Webex Meeting users.

User administrators can also enable or disable the Captions & Highlights panel for their site.

2. Personal Data Processing

The table below lists the personal data processed by Closed Captions to provide its services and describes why the data is processed.

Personal Data Category	Type of Personal Data	Purpose of Processing

Audio Information	• Audio captured during meeting	• Provide Closed Captioning • When you utilize the real time translation and transcription feature in multiple languages, data may be used for product improvement. You may opt-out of this use by submitting a request here.
Transcript Information	• Meeting Transcript • Text of real time speech for translations	• Provide Closed Captioning • When you utilize the real time translation and transcription feature in multiple languages, data may be used for product improvement. You may opt-out of this use by submitting a request here.
Host and Usage Information	• Usage of Closed Captioning features, including number of meetings with Closed Captions enabled, and troubleshooting events	• Provide Closed Captioning • Understand how Closed Captioning is used • Provide Customer with usage information • Diagnose technical issues • Improve the technical performance of the Service

3. Data Center Locations

Webex Closed Captioning data center locations track the data center locations for Webex Assistant, which are outlined in Addendum 4 below. Please refer to Data Center Locations in Addendum 4 below.

4. Cross-Border Data Transfer Mechanisms

Webex Closed Captioning cross-border data transfer mechanisms are the same as those listed for Webex Assistant, which are outlined in Addendum 4 below. Please refer to Addendum 4 below.

5. Access Control

The table below lists the personal data used by Webex Closed Captioning for Meetings, who can access that data, and why.

Personal Data Category	Who has access	Purpose of the access
User Information	Cisco	Enroll users in Closed Captioning.
	Customer	Enable/disable Closed Captioning for specific Webex Meeting users or an entire site
Audio Information	Cisco	While Cisco operates the Service, Cisco will not access this data unless it is shared with Cisco by Customer and will only access in accordance with Cisco's data access and security controls process.

	Customer	Customer will continue to have access to Meeting Recordings (if the meeting was recorded by host) in accordance with Customer's personal data policy and as described in the Meetings Privacy Data Sheet.
	User	No highlights or meeting audio information is retained after the meeting when Close Captioning only is used during the live meeting
Transcript Information	Cisco	While Cisco operates the Service, Cisco will not access this data unless it is shared with Cisco by Customer and will only access in accordance with Cisco's data access and security controls.
	User	By default, no transcript is retained when Closed Captioning only is used during the live meeting unless recording was enabled. If recording was enabled, a transcript will be available in the recording page and review tab in the post meeting experience, a meeting host will be able to view, access and/or share transcript Information. A host may share and give certain edit permissions to other Webex Meetings users.
Host and Usage Information	Cisco	Support and improve the Service in accordance with Cisco's data access and security controls.
	Customer	View and analyze usage information.

6. Data Portability

- Meeting hosts and users with edit privileges to a given meeting can download meeting transcript in txt or vtt formats.
- Meeting hosts and users with edit privileges to a given meeting can email Highlights to a selected email account.
- Meeting hosts and users with edit privileges to a given meeting can share a meeting in an existing or a newly created Webex space

7. Data Deletion and Retention

Subject only to their employer's corporate retention policies, users with an active subscription have control over their Audio and Transcript Information and can delete such information from their account through the My Webex Page as described below. If you have any questions regarding deletion or deletion requests, please contact Cisco through the Cisco Privacy Request Form. .

The table below lists the personal data used by Webex Closed Captioning for Meetings, the length of time that data needs to be retained, and why we retain it.

Type of Personal Data	Retention Period	Reason for Retention
User Information	User Information is not separately stored or retained as part of Closed Captioning,as this information is already	

	stored by Webex Meetings.	
Audio Information	Active Subscriptions: Audio Information deleted at Customer's or user's discretion. Terminated Service: Deleted within 60 days	Audio Information is retained in order to provide you with the Service and will be deleted once it is no longer necessary to provide the Service. Audio Information retained after the Service is terminated is done in order to make it available to Customers for download. Audio Information related to real time translation and transcription in multiple languages is retained for 2 years for product improvement. You may opt-out of this use by submitting a request here.
Transcript Information	Active Subscriptions: Highlights may be deleted at Customer's or user's discretion. Terminated Service: Deleted within 60 days	Transcript Information is retained in order to provide you with the Service and will be deleted once it is no longer necessary to provide the Service. Transcript Information retained after the Service is terminated is done in order to make it available to Customers for download Transcription Information related to real time translation and transcription in multiple languages is retained for 2 years for product improvement. You may opt-out of this use by submitting a request here.
Host and Usage	Deleted after 3 years.	Usage information used to conduct analytics and measure statistical performance is retained but pseudonymized.

8. Personal Data Security

Cisco has implemented appropriate technical and organizational measures designed to secure personal data from accidental loss and unauthorized access, use, alteration, and disclosure.

The table below summarizes encryption architecture of data stored specifically for Closed Captioning.

Personal Data Category	Security controls and measures
User Information	Closed Captioning does not store or retain this information separately than already maintained by Webex Meetings.

Audio Information	Encrypted in transit. Closed Captions are not stored at rest.
Transcript Information	Encrypted in transit. Closed Captions are not stored at rest.
Host and Usage	Encrypted in transit and at rest.

9. Sub-processors

Cisco partners with service providers that act as sub-processors and contract to provide the same level of data protection and information security that you can expect from Cisco. A current list of sub-processors for Closed Captioning is below:

Sub-processor	Personal Data	Service Type	Location of Data Center
Amazon Web Services	Audio Information	Cloud Infrastructure (transient storage only)	US, , Singapore, France, Japan, Ireland, Sweden
Google	Audio and transcript of Voice Command only (e.g., "Ok, Webex, create a note"). Please note that the core transcription technology that processes and stores all other Audio and Transcript Information is owned, managed and executed by Cisco.	• Speech to Text service (voice commands only) • Text to Speech service (voice command responses only)	US, Germany, Singapore, Netherlands, Belgium, Japan
Google*	Transcript Information	Provide translation and/or foreign language transcription using text of real time speech. Google may process but not store transcript Information to provide speech-to-text services Transcript data is processed by Google at global endpoints, except when a Customer is provisioned in the European Union (EU). For EU Customers, transcript data prossessed by Google is processed within region as part of Webex Data Residency.	Globally For EU Customers, within the EU

	Audio Information (except if spoken language chosen is English)	When you add-on and use the real time translation and transcription feature in multiple languages, Google may process but not store Audio Information to provide speech-to-text services Audio data is processed by Google at global endpoints, except when a Customer is provisioned in the European Union (EU). For EU Customers, audio data processed by Google is prossessed within region as part of Webex Data Residency.	Globally For EU Customers, within the EU

*These sub-processors will only apply to You if You have purchased and are using real-time translation and transcription in multiple languages.

Addendum Four: Webex Assistant for Meetings (Optional)

This Addendum describes the processing of personal data (or personal identifiable information) by Webex Assistant for Meetings ("Webex Assistant" or "Assistant") feature for Cisco Webex Meetings.

Webex Assistant for Meetings is a cloud-based feature made available by Cisco to companies or persons who acquire it for use by their authorized users. Webex Assistant provides additional functionality to Closed Captioning, for example allowing users to use voice commands, highlight closed captions during the meeting, and edit or share highlights after a meeting.

Cisco will process personal data from Webex Assistant for Meetings in a manner that is consistent with this Privacy Data Sheet. In jurisdictions that distinguish between Data Controllers and Data Processors, Cisco is the Data Controller for the personal data processed to administer and manage the Customer relationship. Cisco is the Data Processor for the personal data processed by Cisco Webex Meetings in order to provide its functionality.

Note: This Privacy Data Sheet is a supplement to the Cisco Online Privacy Statement.

1. Overview

Webex Assistant for Meetings is an intelligent, interactive virtual meeting assistant that makes meetings searchable, actionable, and more productive. When Webex Assistant is turned on, the meeting host and participants can capture meeting highlights with one click or through a voice command. Even when Webex Assistant joins a Meeting, it will only be activated by the wake word, "OK Webex." Once the wake word is detected, the voice command is streamed to the cloud for speech-to-text transcription and processing. Any participant can use one of many voice commands and create a meeting highlight. Meeting Highlights can include meeting key points, notes, summaries, agendas, action items or decisions.

Webex user administrators can enable or disable Webex Assistant for Meetings for a Webex site and can restrict use of Webex Assistant to certain users or groups of users at any time.

Cisco has put several controls in place to ensure user transparency. When Webex Assistant is enabled, the Webex Assistant icon appears in the lower left of the host and participant's screen. On Webex endpoint devices, there will be a visual cue similar to the existing one you see when a meeting is recorded. Additionally, when the host turns on Webex Assistant in a meeting, there will be an audio announcement made to all participants on the call, even if they join late (unless the Webex user administrator has disabled the announcement). As further described below, the host can choose to share the transcript and meeting highlights with other Webex Meeting users.

2. Personal Data Processing

The table below lists the personal data processed by Webex Assistant for Meetings to provide its services and describes why the data is processed.

Personal Data Category	Type of Personal Data	Purpose of Processing

User Information	• Name (First, Last) • Email • Username • Unique User Identifier (UUID)	• Enable Webex Assistant for specific Webex Meeting users or for an entire site • Provide Webex Assistant
Audio Information	• Meetings Recordings • Audio Commands to Webex Assistant • Audio captured during meeting	• Provide Webex Assistant • When you utilize the real time translation and transcription feature in multiple languages, data may be used for product improvement. You may opt-out of this use by submitting a request here.
Transcript Information	• Meeting Transcript • Text of meeting Highlight • Text of real time speech for translations	• Provide Webex Assistant • When you utilize the real time translation and transcription feature in multiple languages, data may be used for product improvement. You may opt-out of this use by submitting a request here.
Host and Usage Information	• Usage of the Webex Assistant features, including number of meetings with Assistant enabled, number/type of Highlight views/edits/downloads, troubleshooting events	• Provide Webex Assistant • Understand how Webex Assistant is used • Provide Customer with usage information • Diagnose technical issues • Improve the technical performance of the Service

3. Data Center Locations

Cisco leverages its own data centers as well as third-party hosting providers and business partners to deliver the Service, including Webex Assistant, globally.

Webex Assistant Audio and Transcript Information will be stored in the same location in which the Customer is provisioned for Webex Meeting recordings. Although Webex Assistant may process data in AWS as listed in Section 9 below, no data will be stored there.

4. Cross-Border Data Transfer Mechanisms

Cisco has invested in transfer mechanisms to enable the lawful use of data across jurisdictions:

- Binding Corporate Rules (Controller)
- APEC Cross-Border Privacy Rules
- APEC Privacy Recognition for Processors
- EU Standard Contractual Clauses

5. Access Control

The table below lists the personal data used by Webex Assistant for Meetings, who can access that data, and why.

Personal Data Category	Who has access	Purpose of the access
User Information	Cisco	Enroll users with Webex Assistant.
	Customer	Enable Webex Assistant for specific Webex Meeting users or for an entire site
Audio Information	Cisco	While Cisco operates the Service, Cisco will not access this data unless it is shared with Cisco by Customer and will only access in accordance with Cisco's data access and security controls process.
	Customer	Customer will continue to have access to Meeting Recordings in accordance with Customer's personal data policy and as described in the Meetings Privacy Data Sheet.
	User	A meeting host will be able to view, access and/or delete highlights. A host may share and give certain edit permissions to other Webex Meetings users.
	Cisco	While Cisco operates the Service, Cisco will not access this data unless it is shared with Cisco by Customer and will only access in accordance with Cisco's data access and security controls.
	User	A meeting host will be able to view, access and/or share transcript Information. A host may share and give certain edit permissions to other Webex Meetings users.
	Cisco	Support and improve the Service in accordance with Cisco's data access and security controls.

6. Data Portability

Users have the option to email any transcript or highlight to a selected email account.

7. Data Deletion and Retention

Subject only to their employer's corporate retention policies, users with an active subscription have control over their Audio and Transcript Information and can delete such information from their account through the My Webex Page as described below. If you have any questions regarding deletion or deletion requests, please contact Cisco through the Cisco Privacy Request Form. .

The table below lists the personal data used by Webex Assistant for Meetings, the length of time that data needs to be retained, and why we retain it.

Type of Personal Data	Retention Period	Reason for Retention
User Information	User Information is not separately stored or retained by Webex Assistant as this information is already stored by Webex Meetings.	
Audio Information	Active Subscriptions: Audio Information deleted at Customer's or user's discretion. Terminated Service: Deleted within 60 days	Audio Information is retained in order to provide you with the Service and will be deleted once it is no longer necessary to provide the Service. Audio Information retained after the Service is terminated is done in order to make it available to Customers for download. Audio Information related to real time translation and transcription in multiple languages is retained for 2 years for product improvement. You may opt-out of this use by submitting a request here.
Transcript Information	Active Subscriptions: Highlights may be deleted at Customer's or user's discretion. Terminated Service: Deleted within 60 days	Transcript Information is retained in order to provide you with the Service and will be deleted once it is no longer necessary to provide the Service. Transcript Information retained after the Service is terminated is done in order to make it available to Customers for download Transcription Information related to real time translation and transcription in multiple languages is retained for 2 years for

		product improvement. You may opt-out of this use by submitting a request here.
Host and Usage	Deleted after 3 years.	Usage information is used to conduct analytics and measure statistical performance.

8. Personal Data Security

Cisco has implemented appropriate technical and organizational measures designed to secure personal data from accidental loss and unauthorized access, use, alteration, and disclosure.

The table below summarizes encryption architecture of data stored specifically for Webex Assistant.

Personal Data Category	Security controls and measures
User Information	Webex Assistant does not store or retain this information separately than already maintained by Webex Meetings.
Audio Information	Encrypted in transit and at rest.
Transcript Information	Encrypted in transit and at rest.
Host and Usage	Encrypted in transit and at rest.

9. Sub-processors

Cisco partners with service providers that act as sub-processors and contract to provide the same level of data protection and information security that you can expect from Cisco. A current list of sub-processors for Webex Assistant is below:

Sub-processor	Personal Data	Service Type	Location of Data Center
Amazon Web Services	Audio Information	Cloud Infrastructure (transient storage only)	US, , Singapore, France, Japan, Ireland, Sweden

Google	Audio and transcript of Voice Command only (e.g., "Ok, Webex, create a note"). Please note that the core transcription technology that processes and stores all other Audio and Transcript Information is owned, managed and executed by Cisco.	• Speech to Text service (voice commands only) • Text to Speech service (voice command responses only)	US, Germany, Singapore, Netherlands, Belgium, Japan
Google*	Transcript Information	Provide translation using text of real time speech. This may be retained up to 14 days in case of service failure but will not be used other than to provide you with Webex Assistant. Transcript data is processed by Google at global endpoints, except when a Customer is provisioned in the European Union (EU). For EU Customers, transcript data prossessed by Google is processed within region as part of Webex Data Residency.	Globally For EU Customers, within the EU
	Audio Information (except if spoken language chosen is English)	When you add-on and use the real time translation and transcription feature in multiple languages, Google may process but not store Audio Information to provide speech-to-text services Audio data is processed by Google at global endpoints, except when a Customer is provisioned in the European Union (EU). For EU Customers, audio data processed by Google is prossessed within region as part of Webex Data Residency.	Globally For EU Customers, within the EU

*These sub-processors will only apply to you if you have purchased and are using real-time translation and transcription in multiple languages.

Addendum Five: Webex Assistant for Rooms

This Addendum describes the processing of personal data (or personal identifiable information) by Webex Assistant for Rooms.

Webex Assistant for Rooms is a cloud-based feature made available by Cisco to companies or persons who acquire it for use by their authorized users.

Cisco will process personal data from Webex Assistant for Rooms in a manner that is consistent with this Privacy Data Sheet. In jurisdictions that distinguish between Data Controllers and Data Processors, Cisco is the Data Controller for the personal data processed to administer and manage the Customer relationship. Cisco is the Data Processor for the personal data processed by Cisco Webex Meetings in order to provide its functionality.

1. Overview

Webex Assistant for Rooms gives you a new way to control your devices by using voice commands. Through voice commands, a user is able to join meetings, control meeting settings and more. Webex Assistant is disabled by default and can be enabled by the Organization's administrator in Webex Control Hub.

Webex Assistant is activated by the wake word, "OK Webex." Once the wake word is detected, speech is streamed to the cloud for speech-to-text transcription. As wake word processing is local on the device, no audio data is stored, processed or streamed to the cloud until the wake word is detected. After the wake word and command are processed, the resulting text from the speech engine is returned to the Webex Assistant client on the endpoint device and displayed to the user. Although Webex Assistant for Rooms securely manages functional interactions with Google Speech Services to enable the service, data is not stored or further processed by Google for any other purpose than to provide you with the service.

2. Personal Data Processing

The table below lists the personal data processed by Webex Assistant for Rooms to provide its services and describes why the data is processed.

Personal Data Category	Type of Personal Data	Purpose of Processing

User Information	• Synched Corporate Directory information (e.g., name, email, title)
	• For users who pair with Cisco endpoint device:
	  ○ Unique User Identifier
	  ○ First Name
	  ○ Display name
		• Provide Webex Assistant
		• Improve Webex Assistant's accuracy to user's command

Audio	• User audio commands	• Provide Webex Assistant
Transcripts	• Text of command	• Provide Webex Assistant • Train and/or improve Cisco language services
Usage	• Webex Assistant usage information (e.g., number of queries from endpoint devices, dates) • Endpoint devices used	• Understand how Webex Assistant is used • Diagnose technical issues • Improve the technical performance of Webex Assistant

3. Data Center Locations

Cisco leverages its own data centers as well as third-party hosting providers and business partners to deliver Webex Assistant for Rooms globally. These entities are currently located in the following locations (data center locations may change from time to time and this Privacy Data Sheet will be updated to reflect those changes):

Data Center Locations
Germany
United States

4. Cross-Border Data Transfer Mechanisms

Cisco has invested in transfer mechanisms to enable the lawful use of data across jurisdictions:

- Binding Corporate Rules (Controller)
- APEC Cross-Border Privacy Rules
- APEC Privacy Recognition for Processors
- EU Standard Contractual Clauses

5. Access Control

The table below lists the personal data used by Webex Assistant for Rooms, who can access that data, and why.

Personal Data Category	Who has access	Purpose of the access
User Information	Cisco	Enable, support and improve Webex Assistant in accordance with Cisco's data access and security controls process.
Audio	Cisco	Provide Webex Assistant
Transcripts	Cisco	Support, train and improve Webex Assistant. Understand how the product is being used.
Usage Information	Cisco	Support and improve the Service in accordance with Cisco's data access and security controls process. Understand how the product is being used.
	Customer	View and analyze some usage information on Control Hub.

6. Data Portability

While Webex Meetings allows Customers and users to export data as described in Section 5 of the Webex Meetings Data Privacy Sheet, it does not support the export of Webex Assistant for Rooms data.

7. Data Deletion and Retention

The table below lists the personal data used by Webex Assistant for Rooms, the length of time that data needs to be retained, and why we retain it.

Type of Personal Data	Retention Period	Reason for Retention
User Information	Stored while Customer is enrolled in Webex Assistant for Rooms. After Customer disables Webex Assistant, User Information is deleted within a week. If you have paired with a device, the relevant data is retained for 1 year.	User Information is retained in order to provide you with the service and will be deleted once it is no longer necessary to provide the service.
Audio	Not retained	N/A
Transcript	2 years	Transcripts are retained to evaluate and improve Webex Assistant and understand how the product is being used. Text transcripts containing no personal data (e.g., "OK Webex, Start a Meeting") will be de- identified and may be stored indefinitely.

Usage	Deleted within 1 year	Usage is retained to evaluate the service and understand how Webex Assistant is being used.

8. Personal Data Security

Cisco has implemented appropriate technical and organizational measures designed to secure personal data from accidental loss and unauthorized access, use, alteration, and disclosure.

The table below summarizes encryption architecture of data stored specifically for the Webex Assistant for Rooms.

Personal Data Category	Security controls and measures
User Information	Encrypted in transit, encrypted at rest
Audio	Encrypted in transit, no storage at rest
Transcript	Encrypted in transit, encrypted at rest
Usage	Encrypted in transit, encrypted at rest

9. Sub-processors

Cisco partners with service providers that act as sub-processors and contract to provide the same level of data protection and information security that you can expect from Cisco. A current list of sub-processors for Webex Assistant for Rooms is below:

Sub-processor	Personal Data	Service Type	Location of Data Center
Google Cloud	Audio	Speech to text service	Worldwide
Google Cloud	• Transcript • Usage	Cloud storage region	United States
Splunk	• Transcript • Usage	Data analysis platform	United States

Addendum Six: Slido in Webex (Optional)

This Addendum to the Webex Meetings Privacy Data Sheet describes the processing of personal data (or personally identifiable information) by the Slido feature in Webex ("Slido," "Slido in Webex," or the "Service").

1. Overview of Slido in Webex Meetings Capabilities

Slido in Webex is a cloud-based polling and Q&A solution aimed at B2B customers. Users stay engaged during meetings by voting in live polls and asking questions. Slido is an integrated part of Webex Meetings or available to hosts and meeting participants as a web application. For a detailed overview of the Service, please visit the Slido in Webex website.

2. Personal Data Processing

Because of the nature of the Service, we do not expect any sensitive data to be sent through Slido.

The table below lists the personal data processed by Slido in Webex to provide its services and describes why the data is processed.

Personal Data Category	Type of Personal Data	Purpose of Processing
Host Information	• Name, email address, organization ID	We use this data to: • Provide the service (may include support, maintenance, and protection of the service)
Participant Information	• Name, email address, organization ID	We use this data to: • Provide the service
User Generated Information	• Questions, polls, answers, ideas, chats - any content shared or created by participants and hosts	We use this data to: • Provide the service
User Technical Information	• Device data (e.g. hardware model, operating system version, unique device identifiers), • Log data (e.g. your search queries, details about your connection such as IP address, date, time, edge-location, ssl-protocol, ssl-cipher or time- taken to serve you requested site, device event information such	We use this user technical data: • For the purposes of providing, tailoring and improvement of the service

	as crashes, system activity, hardware settings, browser type, browser language, the date and time of your request and referral URL) • Location information (IP address) • Unique users IDs • browser local storage and application data caches	
Cookies	• Essential cookies collected through embedded browser utilized in the Webex-Slido interface	We use cookies: • To provide, tailor and improve the service

Support Information	We collect contact data of people reaching out through Slido.com for support: • Usually name, email, company	We use contact data of people reaching out to us: • Providing Support • Tailoring and improvement of our service

Technical Support Assistance

If a Customer reaches out to Cisco Technical Assistance Center (TAC) for problem diagnosis and resolution, Cisco TAC may receive and process personal data from the Service. The Cisco TAC Service Delivery Privacy Data Sheet describes Cisco's processing of such data.

3. Data Center Locations

Cisco uses third-party infrastructure providers to deliver the service globally. Please see Section 8 for a list of subprocessors, including infrastructure providers.

Data Center Locations
Ireland
Germany

4. Cross-Border Data Transfer Mechanisms

Cisco has invested in transfer mechanisms to enable the lawful use of data across jurisdictions:

- Binding Corporate Rules (Controller)
- APEC Cross-Border Privacy Rules
- APEC Privacy Recognition for Processors
- EU Standard Contractual Clauses

5. Access Control

The table below lists the personal data used by Slido in Webex to carry out the service, who can access that data, and why. Content you choose to share during an event may be accessed by users in the event, wherever they are located. Even after you remove information from the Service, copies of that content may remain viewable elsewhere to the extent it has been shared with others.

Personal Data Category	Who has access	Purpose of the access
Host Information	Host	View host profile data through slido.com

	Customer	Manage, delete user's slido profiles through slido.com
	Cisco	Provide the service
Participant Information	Host	View joined participants through slido.com
	Cisco	Support the service in accordance with Cisco's data access and security controls
	Customer	Delete participant content data by submitting privacy request form
	Host	View submitted User Generated Information through slido.com
	Cisco	Support the service in accordance with Cisco' data access and security controls. Cisco will not access this data unless an authorization is granted by the Customer, and will only access it in accordance with Cisco's data access and security controls.
	Cisco	Provide, tailor and improve the service
	Cisco	Provide, tailor and improve the service
	Cisco	Support Information is kept as part of record of service delivery

6. Data Portability

Slido allows Customers and hosts to export event content data through slido.com.

7. Data Deletion and Retention

The table below lists the personal data used by Slido, the length of time that data needs to be retained, and why we retain it.

Type of Personal Data	Retention Period	Reason for Retention
Host Information	Host Information is retained until account termination.	• Provide the service
Participant Information	Participant Information associated with a specific meeting is retained until account termination. Participant Information associated with a specific meeting can be deleted by deleting all Slido data	• Provide the service

	associated with that meeting. As request must be submitted through a privacy request.	
User Generated Information	User Generated Information associated with a specific meeting is retained until account termination.	• Provide the service

	User Generated Information associated with a specific meeting can be deleted by deleting all Slido data associated with that meeting. As request must be submitted through a privacy request.	
Technical Information	Deleted 1 year after collection	• Technical Information is kept as part of Cisco's record of service delivery, conduct analytics and measure statistical performance.
Cookies	Maximum of one year	• To provide, tailor and improve the service
Support Information	Not deleted	• Support Information is kept as part of record of service delivery.

8. Personal Data Security

Slido has implemented appropriate technical and organizational measures designed to secure personal data from accidental loss and unauthorized access, use, alteration, and disclosure.

Personal Data Category	Security controls and measures
Host Information	Encrypted in transit and at rest
Participant Information	Encrypted in transit and at rest
User Generated Information	Encrypted in transit and at rest
User Technical Information	Encrypted in transit and at rest
Cookies	Encrypted in transit and at rest
Support Form Information	Encrypted in transit

9. Sub-processors

Cisco partners with service providers that act as sub-processors and contract to provide the same level of data protection and information security that you can expect from Cisco. A current list of sub-processors for the service is below:

Sub-processor	Personal Data	Service Type	Location of Data Center
Amazon Web Services	• Host Information • Participant Information • User-Generated Information	Infrastructure as a Service	Dublin, Ireland Frankfurt, Germany

	• User Technical Information • Cookies • Support Information		

10. Information Security Incident Management

Breach and Incident Notification Processes

The Data Protection & Privacy team within Cisco's Security & Trust Organization coordinates the Data Incident Response Process and manages the enterprise-wide response to data-centric incidents. The Incident Commander directs and coordinates Cisco's response, leveraging diverse teams including the Cisco Product Security Incident Response Team (PSIRT), the Cisco Security Incident Response Team (CSIRT), and the Advanced Security Initiatives Group (ASIG).

PSIRT manages the receipt, investigation, and public reporting of security vulnerabilities related to Cisco products and networks. The team works with Customers, independent security researchers, consultants, industry organizations, and other vendors to identify possible security issues with Cisco products and networks. The Cisco Security Center details the process for reporting security incidents.

The Cisco Notification Service allows Customers to subscribe and receive important Cisco product and technology information, including Cisco security advisories for critical and high severity security vulnerabilities. This service allows Customers to choose the timing of notifications, and the notification delivery method (email message or RSS feed). The level of access is determined by the subscriber's relationship with Cisco. If you have questions or concerns about any product or security notifications, contact your Cisco sales representative.

11. Certifications and Compliance with Privacy Requirements

The Security & Trust Organization and Cisco Legal provide risk and compliance management and consultation services to help drive security and regulatory compliance into the design of Cisco products and services. The Service is built with privacy in mind and is designed so that it can be used in a manner consistent with global privacy requirements.

In addition to the Cross-Border Data Transfer Mechanisms/Certifications listed in Section 4, Cisco has the following:

- EU-US Privacy Shield Framework Swiss-US Privacy Shield Framework
-

Further, in addition to complying with our stringent internal standards, Cisco also maintains third-party validations to demonstrate our commitment to information security.

Slido in Webex currently holds the following privacy certifications:

- ISO27001

As part of its integration, Slido in Webex intends to pursue other privacy certifications, including those associated with Webex.

12. Exercising Data Subject Rights

Users whose personal data is processed by the Service have the right to request access, rectification, suspension of processing, or deletion of the personal data processed by the Service.

We will confirm identification (typically with the email address associated with a Cisco account) before responding to the request. If we cannot comply with the request, we will provide an explanation. Please note, users whose employer is the Customer/Controller, may be redirect to their employer for a response.

Requests can be made by submitting a request via:

1) the Cisco Privacy Request form
2) by postal mail:

Chief Privacy Officer Cisco Systems, Inc. 170 W. Tasman Drive San Jose, CA 95134 UNITED STATES		
Americas Privacy Officer Cisco Systems, Inc. 170 W. Tasman Drive San Jose, CA 95134 UNITED STATES	APJC Privacy Officer Cisco Systems (USA) Pte Ltd Bldg 80, Lvl 25, Mapletree Biz City, 80 Pasir Panjang Road, Singapore, 117372 SINGAPORE	EMEAR Privacy Officer Cisco Systems, Inc. Haarlerbergweg 13-19, 1101 CH Amsterdam-Zuidoost NETHERLANDS

We will endeavor to timely and satisfactorily respond to inquiries and requests. If a privacy concern related to the personal data processed or transferred by Cisco remains unresolved, contact Cisco's US-based third-party dispute resolution provider.

Alternatively, you can contact the data protection supervisory authority in your jurisdiction for assistance. Cisco's main establishment in the EU is in the Netherlands. As such, our EU lead authority is the Dutch Autoritiet Persoonsgegevens.

Addendum Seven: Cisco-Developed Embedded Apps (Optional)

This Addendum to the Webex Meetings Privacy Data Sheet describes the processing of personal data (or personally identifiable information) by Cisco-developed embedded apps in Webex Meetings. Embedded apps developed by third parties, as stated in the Webex Meetings Privacy Data Sheet, are governed by the respective third party's privacy policies.

Shared Timer

1. Overview

Shared Timer (the "Service") is a cloud-based application that allows meeting hosts and participants to set a timer, using preset intervals, during a particular meeting. The countdown timer is displayed with other meeting participants.

Personal data processing for Shared Timer is largely covered by the disclosed personal data processing associated with the Webex Meetings Service; for that, please refer to the Webex Meetings Privacy Data Sheet above.

A Customer user administrator controls whether user-level personal data can be shared with Shared Timer. In Control Hub, the Customer user administrator can set enable or disable PII sharing through "PII Restrictions." "PII restrictions" are disabled by default (i.e., without any action by Customer user administrator) and the only pseudonymized user-level personal data will be processed by Shared Timer, as described below.

The following information is supplementary privacy data information associated specifically with Shared Timer.

2. Personal Data Processing

The table below lists the personal data processed by Shared Timer to provide its services and describes why the data is processed.

If PII restrictions are enabled, PII sharing mode is on, and the following applies:
To the extent personal data is shared with sub-processors, it is encrypted at transit. Sub-processors do not have access to the data in the raw.

Personal Data Category	Type of Personal Data	Purpose of Processing
User Information	• UUID • Display Name	• UUID used to identify which user within the meeting performed specific activities (e.g., who paused the timer); • Display Name is processed to identify the user-specific activities

		(to display that a certain individual set or reset the timer)
Host and Usage Information*	• IP Address • User Agent • Browser • Operating System • Device Type	• Provide you with the Service • Understand how the Service is used Diagnose technical issues • Conduct analytics and statistical analysis in aggregate form to improve the technical performance of the Service • Respond to Customer support requests • Make improvements to the Service and other Cisco products and services.

If the PII restrictions are disabled, PII sharing is off, and the following applies:

Personal Data Category	Type of Personal Data	Purpose of Processing
User Level	• Personal data that is collected (e.g., UUID and Display Name) is pseudonymized	• UUID used to identify which user within the meeting performed specific activities (e.g., who paused the timer); • Name is processed to identify the user- specific activities (to display that a certain individual set or reset the timer)
Host and Usage Information*	• IP Address • User Agent • Browser • Operating System • Device Type	• Provide you with the Service • Understand how the Service is used • Diagnose technical issues • Conduct analytics and statistical analysis in aggregate form to improve the technical performance

		of the Service • Respond to Customer support requests • Make improvements to the Service and other Cisco products and services.

2. Sub-processors

Shared Timer does not use the sub-processors listed in the Webex Meetings Privacy Data Sheet. Shared Timer uses only the following third-party sub-processor.

Sub-processor	Personal Data	Service Type	Location of Data Center
Amazon Web Services	UUID[1] Display Name[2]	Used to provide Shared Timer functionality	USA

[1]Collected through use of Webex Meetings processed in connection with Shared Timer

[2]When PII sharing mode is ON. When PII sharing mode if OFF, data is pseudonymized

EXHIBIT D

ATTACHMENT 2 - TAC PRIVACY DATA SHEET

Cisco Technical Assistance (TAC) Service Delivery

This Privacy Data Sheet describes the processing of personal data (or personally identifiable information) by Cisco TAC

Cisco will process personal data from customers in a manner that is consistent with this Privacy Data Sheet. In jurisdictions that distinguish between Data Controllers and Data Processors, Cisco is the Data Controller for the personal data processed to administer and manage the customer relationship. Cisco is the Data Processor for the personal data processed by Cisco TAC in order to provide its functionality.

Note: This Privacy Data Sheet is a supplement to the Cisco Online Privacy Statement.

15. Overview

Cisco's Support Services Technical Assistance Center (TAC) is a global organization that provides around-the-clock, award-winning technical support services online and over the phone. TAC offers customer support for all Cisco products/services using a global follow-the-sun support model. Our TAC teams support thousands of service requests every day, as well as supply best-in-class hardware support, repair, and replacement from one of our 1,100 depots.

As part of our TAC services support process, service requesters may be required to provide certain personal data. These data are limited to business contact details provided by the requester and used for the purposes of providing the support required.

Customer Case Attachment Data (including text, audio, video or image files), which are provided to Cisco by a customer in connection with the customer's use of Cisco products or services, or data developed by Cisco at the specific request of a customer, is subject to the following security controls:

i. Authentication
ii. Access control
iii. Login/activity logging and monitoring
iv. Data masking
v. Data encryption, both at rest and in transit
vi. Transport and storage for physical data

For more general information related to Cisco's Technical Services, please visit Cisco.com.

16. Personal Data Processing

The table below lists the personal data processed by Cisco TAC to provide its services and describes why the data is processed.

Personal Data Category	Type of Personal Data	Purpose of Processing
TAC Support Information	• Name • Email Address • Phone Number of the Employee Appointed to Open the Service Request • Authentication Information (exclusive of passwords) • Work organization and responsibilities • Current employer name	We use TAC Support Information to: • Provide remote access support • Review quality of the support service • Perform analysis of the service solution
Customer Case Attachment	Cisco TAC does not intentionally collect or process personal data via Customer Case Attachments. We instruct customers to provide the least amount of personal data possible. However, unsolicited personal data may be contained in the files provided by customers. For illustrative purposes only, the list below includes the types of data that may be processed for Customer Case Attachments for the purpose of providing support: • Device Configuration (e.g., running config and startup config, SNMP Strings (masked); Interface description • Command Line Interface (CLI) (i.e., Show Commands, such as Show Version) • Product Identification Numbers • Serial Numbers • Host Names • Sysdescription (has device location) • IP Addresses • Operating System (OS) Feature Sets • OS Software Versions • Hardware Versions • Installed Memory • Installed Flash • Boot Versions • Chassis Series	We use Customer Case Attachments to: • Provide remote access support • Perform analysis of the service solution

	• Slot IDs • Card Types • Card Families • Firmware Versions • MAC Address • SNMP MIBs (ACLs, CDP)	

17. Data Center Locations

Cisco TAC leverages a Customer Relationship Management (CRM) case management system to deliver our services and capture TAC Support Information. This system is a customized instance on the SalesForce.com (SFDC) platform known as Support Case Manager (SCM) and utilizes a numerical Service Request (SR) case assignment process. Cisco TAC SR case details and associated case notes within Cisco's CRM system are stored at the Salesforce.com (SFDC) data center, which physically resides in Washington DC, USA.

Customer Case Attachments (including detailed system logs, etc.) uploaded by customers are housed in a data repository hosted by Amazon Web Services (AWS - US East Region, Northern Virginia), and replicated for resiliency to another AWS data repository (AWS - US West Region - Oregon). The AWS instance, known internally as CX Files, maintains robust data security and governance controls, including authentication, authorization, role-based access controls, encryption in transit and at rest, login logging and monitoring, and activity logging and monitoring. CX Files is wholly maintained by the Cisco Customer Care IT / Crypto team and the storage location is not shared with any other AWS customers, nor with any other team within Cisco.

Infrastructure Provider Locations
Amazon Web Services (AWS) - US East (Northern Virginia) Region
Amazon Web Services (AWS) - US West (Oregon) Region
SalesForce.com (SFDC) – Washington D.C., USA

18. Cross-Border Data Transfer Mechanisms

Cisco has invested in transfer mechanisms to enable the lawful use of data across jurisdictions:

i. Binding Corporate Rules (Controller)
ii. APEC Cross-Border Privacy Rules
iii. APEC Privacy Recognition for Processors
iv. EU Standard Contractual Clauses

19. Access Control

The table below lists the personal data used by Cisco TAC to carry out the service, who can access that data, and why.

Personal Data Category	Who has access	Purpose of the access

Cisco TAC Support Information	Customer/Partner	Work with Cisco to resolve their support case
	Cisco Support Personnel	Work with Customer to resolve their support case. Access based on functional responsibility.
Customer Case Attachments	Customer/Partner	Work with Cisco to resolve their support case
	Cisco Support Personnel	Work with Customer to resolve their support case. Access based on functional responsibility.

20. Data Portability

Cisco TAC allows customers to export both their Service Request (SR) case data and Case Attachments related to cases for which they have been granted access. Partners who have been enabled by the customer and assigned to a specific contract, may also view, upload and/or download data on the customer's behalf.

21. Data Deletion and Retention

The table below lists the personal data used by Cisco TAC the length of time that data needs to be retained, and why we retain it.

Type of Personal Data	Retention Period	Reason for Retention
TAC Support Information and Customer Case Attachments	10 Years + 1 day	To ensure efficient support in case of recurring issues and to comply with Cisco audit policies related to business records of services provided to Customers (i.e., legitimate business purposes).

22. Personal Data Security

Cisco has implemented appropriate technical and organizational measures designed to secure personal data from accidental loss and unauthorized access, use, alteration, and disclosure.

Personal Data Category	Security controls and measures
TAC Support Information	• Data encryption, in transit • Authentication • Access control
	• Login/activity logging and monitoring • Data masking
Customer Case Attachments	• Data encryption, both at rest and in transit • Authentication • Access control • Login/activity logging and monitoring • Data masking

23. Sub-processors

Cisco partners with service providers that act as sub-processors and contract to provide the same level of data protection and information security that you can expect from Cisco. A current list of sub-processors for the service is below:

Sub-processor	Personal Data	Service Type	Location of Data Center
Salesforce.com (USA)	TAC Support information	Hosting/Storage	Washington, D.C., USA

24. Information Security Incident Management

Breach and Incident Notification Processes

The Data Protection & Privacy team within Cisco's Security & Trust Organization coordinates the Data Incident Response Process and manages the enterprise-wide response to data-centric incidents. The Incident Commander directs and coordinates Cisco's response, leveraging diverse teams including the Cisco Product Security Incident Response Team (PSIRT), the Cisco Security Incident Response Team (CSIRT), and the Advanced Security Initiatives Group (ASIG).

PSIRT manages the receipt, investigation, and public reporting of security vulnerabilities related to Cisco products and networks. The team works with Customers, independent security researchers, consultants, industry organizations, and other vendors to identify possible security issues with Cisco products and networks. The Cisco Security Center details the process for reporting security incidents.

The Cisco Notification Service allows Customers to subscribe and receive important Cisco product and technology information, including Cisco security advisories for critical and high severity security vulnerabilities. This service allows Customers to choose the timing of notifications, and the notification delivery method (email message or RSS feed). The level of access is determined by the subscriber's relationship with Cisco. If you have questions or concerns about any product or security notifications, contact your Cisco sales representative.

25. Certifications and Compliance with Privacy Requirements

The Security and Trust Organization and Cisco Legal provide risk and compliance management and consultation services to help drive security and regulatory compliance into the design of Cisco products and services. The Service is built with privacy in mind and is designed so that it can be used in a manner consistent with global privacy requirements.

In addition to the Cross-Border Data Transfer Mechanisms/Certifications listed in Section 4, Cisco has the following:

i. EU-US Privacy Shield Framework
ii. Swiss-US Privacy Shield Framework

Further, in addition to complying with our stringent internal standards, Cisco also maintains third-party validations to demonstrate our commitment to information security. Cisco Customer Experience (CX) has received the following certifications:

iii. ISO/IEC 27001:2013

26. Exercising Data Subject Rights

Users whose personal data is processed by the Service have the right to request access, rectification, suspension of processing, or deletion of the personal data processed by the Service.

We will confirm identification (typically with the email address associated with a Cisco account) before responding to the request. If we cannot comply with the request, we will provide an explanation. Please note, users whose employer is the Customer/Controller, may be redirect to their employer for a response.

Requests can be made by submitting a request via:

- the Cisco Privacy Request form
- by postal mail:

<table>
<tr><td colspan="3">Chief Privacy Officer Cisco Systems, Inc. 170 W. Tasman Drive
San Jose, CA 95134
UNITED STATES</td></tr>
<tr><td>Americas Privacy Officer
Cisco Systems, Inc.
170 W. Tasman Drive

San Jose, CA 95134

UNITED STATES</td><td>APJC Privacy Officer
Cisco Systems, Inc.
Bldg 80, Lvl 25, Mapletree Biz City,
80 Pasir Panjang Road,

Singapore, 117372
SINGAPORE</td><td>EMEAR Privacy Officer
Cisco Systems, Inc.
Haarlerbergweg 13-19, 1101 CH

Amsterdam-Zuidoost
NETHERLANDS</td></tr>
</table>

We will endeavor to timely and satisfactorily respond to inquiries and requests. If a privacy concern related to the personal data process or transferred by Cisco remains unresolved, contact Cisco's US-based third-party dispute resolution provider. Alternatively, you c contact the data protection supervisory authority in your jurisdiction for assistance. Cisco's main establishment in the EU is in t Netherlands. As such, our EU lead authority is the Dutch Autoritiet Persoonsgegevens.

27. General Information

For more general information and FAQs related to Cisco's Security and Privacy Program please visit The Cisco Trust Center.

Cisco Privacy Data Sheets are reviewed and updated on an annual, or as needed, basis. For the most current version, go to the Perso Data Privacy section of the Cisco Trust Portal.

DATA TRANSFER IMPACT ASSESSMENT FOR THE USE OF CISCO WEBEX BY THE COURT OF JUSTICE OF THE EUROPEAN UNION

Contents

I. INTRODUCTION

1. The European Data Protection Supervisor ("EDPS") adopted its decision to temporarily authorise the use of ad hoc contractual clauses between the Court of Justice of the EU ("CJEU" or "the Court") and Cisco for transfers of personal data in the CJEU's use of Cisco Webex and related services on August 31, 2021 (case 2021-0255) ("the decision").

2. The decision sets out 14 conditions that the CJEU and Cisco are to meet for the renewal of the authorisation within one year from the date of the decision.

3. As one of the conditions, the EDPS imposed that the CJEU conducts a transfer impact assessment, in particular with regard to personal data collected and processed in the use of Cisco Technical Assistance (TAC) Service Delivery services, as well as Webex App data, for which transfers might still occur.

4. The transfer impact assessment is conducted where necessary with Cisco's assistance, to establish the gaps that need to be filled in the level of protection provided by the current contractual clauses and by the model of the new SCCs for transfers under the GDPR as adapted to Regulation (EU) 2018/1725.

5. The Court should, furthermore, consider all examples of supplementary measures in Annexe 2 of the EDPB Recommendations 01/2020, to identify which supplementary measures would be necessary and appropriate to implement for transfers in the Court's use of Cisco Webex Meeting and related services.

6. The present transfer impact assessment covers nevertheless all transfers of personal data that might occur with the use of Webex, Webex App or Cisco Technical Assistance (TAC).

7. As such, it also identifies in detail and without ambiguities, which personal data from which services will be transferred (including by remote access) for which purpose to which recipients in which third country with which safeguards and measures, in accordance with the first requirement of the EDPS in its decision.

II. DESCRIPTION OF THE SERVICE AND DEFINITIONS

8. Webex or the Webex Suite is a cloud videoconferencing service that encompasses several functionalities or elements.

9. Cisco provides the services offered by Webex and consists of several entities. In the contractual relationship with the CJEU, Cisco is represented by Cisco International Limited, a UK-based company, which also acts as a processor. Whenever necessary to understand the data flow or the contractual relationships, the entity within Cisco is identified.

10. The Webex Suite contains the following functionalities and elements relevant for the use by the CJEU:

- Webex Meetings refers to the Webex product that offers videoconference technology.

- Webex Webinars refers to the Webex product that enables seminars and conferences through a videoconference with a larger number of participants. This product was formerly named 'Webex Events'.

- Webex Events (formerly known as "Socio") refers to the Webex product that allows the organisation of in-person, hybrid, and virtual events. CJEU does not envisage the use of Webex Events.

- Webex Calling allows users to make calls by using the Cloud infrastructure. The CJEU uses, however, Cisco Jabber for internal calls, without the use of a cloud infrastructure. Webex Calling is thus disabled at the CJEU.

- Webex Messaging allows users to send messages by using the Cloud infrastructure. The CJEU uses, however, Cisco Jabber for internal messages, without the use of a cloud infrastructure. Webex Messaging is thus disabled at the CJEU.

- Slido refers to the Cisco product that provides polling, quizzes or other feedback during a videoconference. Use of Slido as an integrated tool in Webex is blocked by the CJEU.

11. The Webex App, installed on the user's computer, provides the integration of Calling, Meetings and Messaging in a single application. The Webex App also allows for the use of WebEx Zero Trust Security End-to-End encryption and Private Meetings (see below). Full details on Cisco's processing of personal data in connection with the Webex App is found in the publicly available Webex App Privacy Data Sheet, located on the Cisco Trust Portal. However, the Webex App will be used by the CJEU as a means to access Webex Meetings. When Webex App is used to access meetings, given the technical configuration and adjustments Cisco has made, personal data will stay in the EU.

12. The Webex Web App and Webex Meetings Web App, which runs in the browser of the user, are not used by the CJEU, as they are not currently compatible with the use of Private Meetings.

13. The Hybrid Calendar Service allows for an integration between a user's Outlook calendar and their calendar of Webex meetings in the Webex App. It facilitates the organisation of meetings with videoconferencing and the update of information in relation to these meetings.

14. Cisco also offers, as part of Webex, specific options to further protect the content of a videoconference:

    - WebEx Zero Trust Security End-to-End encryption ensures that the media stream is not decrypted by the Cisco Webex cloud. Cisco does not have access to the user-generated content of the videoconference. Cisco does maintain access to User information as well as Host and Usage information.

    - Private Meetings is a function that ensures that meeting media is processed on an on-premise server, instead of the cloud. Cisco maintains access to User Information as well as Host and Usage Information, but cannot access the real-time media processing conducted on premises.

15. The Cisco Technical Assistance Center or TAC offers technical support for the use of Webex. Its use generates a separate data flow.

16. The Cisco Meeting Server is a separate on-premise videoconference solution that is also used by the CJEU. Its use falls outside of the use of Webex, Cisco's cloud-based solutions, and precludes data processing within the Cisco cloud.

17. Cisco uses different terms to refer to various categories of data. Not all types of data in those categories are necessarily processed in all circumstances, and details about these categories are found in Cisco's publicly available Privacy Data Sheets on the Cisco Trust Portal. Currently, Cisco uses the following terms to describe various categories of personal data that may be processed in connection with Webex:

    - User Information: Name, E-mail Address, Password, Browser, Phone Number, Mailing Address, Avatar, User Information Included in Your Directory, Unique User ID (UUID).

    - Host and Usage information: IP Address, User Agent Identifier, Hardware Type, Operating System Type and Version, Client Version, IP Addresses Along the Network Path, MAC Address of Your Client, Service Version, Actions Taken, Geographic Region, Meeting Session Information (e.g. date and time, frequency, average and

actual duration, quantity, quality, network activity, and network connectivity), Number of Meetings, Number of Screen Sharing and NonScreen-Sharing Sessions, Number of Participants, Screen Resolution, Join Method, Performance, Troubleshooting, and Diagnostics Information, Meeting Host Information, Host Name and ID, Meeting Site URL, Meeting Start/End Time, Meeting Title and Call attendee information, including e-mail addresses, IP address, username, phone numbers, room device information.

- User-generated Information: Meeting Recordings, Transcriptions of meeting recordings, Uploaded Files.
- TAC support Information: Name, E-mail Address, Phone Number of the Employee Appointed to Open the Service Request, Authentication Information (exclusive of passwords), Work organisation and responsibilities, Current employer name.
- Customer Case Attachment: files provided by customers that might contain personal data. Cisco TAC does not intentionally collect or process personal data via Customer Case Attachments. Cisco instructs customers to provide the least amount of personal data possible.

18. The controller for the processing operations is the CJEU.

19. The processor, and signatory to the contract, is Cisco International Limited, established in the United Kingdom. Cisco Systems, Inc. is a further processor for specific processing operations, in particular, for the purpose of processing that occurs outside of the EU/EEA and for TAC support.

20. Both entities use sub-processors, which are either different entities within the Cisco group or other entities. The identity of the relevant sub-processors is, where necessary, clarified in the description of the data flows.

III. DATA FLOWS AND TRANSFERS OF PERSONAL DATA

21. The use of Webex as a cloud service leads to the processing of personal data by Cisco and, in some cases, the transfer of personal data outside the EU/EEA.

22. The use of a specific suite (Webex Meeting, Webex Webinar or Webex Events) might change the data flow. For example, the use of Webex Webinar might for example lead to the use of vBrick as a sub-processor. These suites are nevertheless referred to as Webex.

23. Since August 2021, the main data centre where the data from the CJEU is processed is located in Frankfurt, with a back-up data centre in Amsterdam. This change were applied upon request of the CJUE by Cisco and managed by Cisco.

24. Transfers of personal data, through remote access or the use of sub processors, is possible, especially for purposes of technical support or when using specific functions. Transfers can also take place due to specific actions by the end user or user administrator.

25. This analysis will concentrate on the personal data that is subject to a potential transfer outside of the EU/EEA, including through remote access.

26. In accordance with the requirements of the EDPS, the data flow as described is reflected in the ad hoc clauses adopted between the CJEU and Cisco.

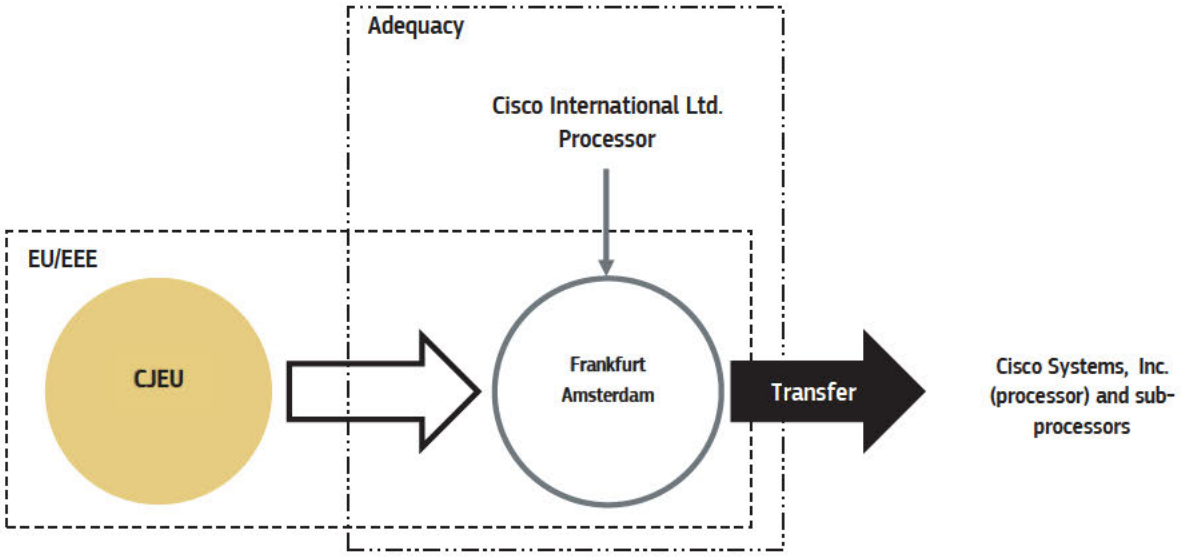
A. Use of Webex

27. The use of Webex leads to the processing of User Information, Host and Usage information and User-Generated Information by the processor. In light of Webex Data Residency for EU customers, the processing largely takes place within the EU/EEA (see Billing, Analytics and Hybrid Calendar Service).

28. Transfers might, however, occur through specific actions or use of functions by the user administrator or user (see User or Admin Actions).

29. Transfers may also take place as a result of the use of third-party sub-processors (see the Use of Third Party Sub-Processors).

30. The data flow can therefore be summarised as such:



1) BILLING

31. Cisco has reviewed its internal processes in order that the processing of personal data required for billing takes place within the EU/EEA for customers provisioned within the EU. No transfer of personal data takes place for billing purposes after July 2022, for customers provisioned within the EU. This is the case for the CJEU.

32. The data used for billing are the host name and e-mail address, the meeting site URL, the Meeting start and end time as well as the telephone number. This data is part of the categories User information and Host and Usage information.

33. The telephone number is processed when applicable. As the CJEU will not provide the telephone numbers of its staff to the processor, the telephone number will not be processed.

34. As the transfer for billing purposes ended in July 2022, specific risks related to this transfer will not be further analysed.

2) ANALYTICS

35. As part of Webex Data Residency, Cisco processes analytics for EU Webex Meetings customers provisioned within the EU/EEA, for all new EU customers and for existing EU customers that perform a migration through Control Hub. This eliminates the transfers of personal data for analytics purposes after July 2022, for customers provisioned within the EU. This also includes transfers following remote access to analytics data.

36. The data used for analytics is User Information and Host and Usage Information. The data is used to provide analytics and statistical analysis in aggregate form (for example, reports prepared for customers to summarise overall Webex usage) and to improve the technical performance of the Service. These reports may contain personal data.

37. As transfers for billing and analytics ended in July 2022, specific risks related to this transfer will not be further analysed.

3) HYBRID CALENDAR SERVICE

38. The use of the Hybrid Calendar Service does not materially alter the data flow, although it does imply the processing of data related to meetings without videoconferencing. A Customer user administrator has the ability to opt into integration with Microsoft 365 (Outlook) for all users across an organisation.

39. The CJEU uses a specific server (ExpressWay Core) hosted at CJUE premises in order to control the transmission of data.

40. The data processed in connection with the Hybrid Calendar Service is, for all meetings planned within a set period (5 days in the past and 30 days in the future), the start and end time and duration of the meeting in the Outlook Calendar, the subject matter and contents of the Outlook invitation (the User-Generated Information associated with Hybrid Calendar Service), as well as the participants' UUID (if Webex users) or e-mail addresses (if guests). The invitation to the meeting is, however, sent by Outlook and not Webex.

41. The User-Generated Information is end-to-end encrypted and not accessible to Cisco, except for the UUID which remains accessible in the logs of the service. With Webex Data Residency, the data is stored in the EU and is not transferred outside the EU for the use of Webex.

4) CUSTOMER, USER, OR USER ADMINISTRATOR ACTIONS

42. Data transfers outside of the EU/EEA may also take place for the following reasons:

    a) a Customer or user registers a user on any Cisco platform (for example, through www.webex.com or www.cisco.com) or through any Cisco service to learn more about Cisco products or events;

    b) a Customer provides ordering information (business contact information);

    c) a user engages in collaboration with users outside of the EU region;

    d) a Customer, user, or user administrator requests technical support through Cisco's Technical Assistance Center ("TAC") (in which case the information that a user provides within the initial TAC request may be transferred outside the region);

    e) a Customer, user, or user administrator enables certain optional functionalities; or a user or user administrator enables cell phone "push" notifications (in which case the cell phone provider associated with iOS or Android functionality may transfer data outside of the region).

43. The CJEU has, however, taken measures to avoid or limit such transfers.

5) USE OF THIRD PARTY SUB-PROCESSORS

44. Cisco uses other sub-processors for some processing of personal data. While sub-processors were included as part of EU Data Residency program, the use of certain sub-processors may lead to a transfer of personal data outside of the EU/EEA in certain circumstances.

    1) Step-by-step Tour and Guidance

45. In order to provide a step-by-step guidance on how to use WebEx online, Cisco uses Walkme, Inc. as a sub-processor. This sub-processor uses the Unique User ID and the user region to provide the service.

46. As part of Cisco's Webex Data Residency program, Walkme, Inc. has taken measures that data from EU customers would be processed in the EU.

47. These services can, however, be turned off by the controller. As the CJEU turned this feature off in the administration console, the processing and any possible related transfer of personal data to the United States (for example through remote access) will not take place.

2) Extended Capacity for WebEx Meetings

48. In order to provide capacity for over 3 000 participants for Webex, Cisco uses Vbrick a sub-processor. This sub-processor uses the Name, Unique User ID and the user region to provide the service. The processing can take place in the EU, the United States or Australia.

49. As part of Cisco's Webex Data Residency program, Vbrick has taken measures that data from EU customers would be processed in the EU.

50. Furthermore, the license of the CJEU for the use of Webex is limited to 1 000 participants for a meeting. To the extent the meetings organised by the CJEU are limited to a maximum of 1 000 participants, Vbrick is not implicated in the data processing.

3) Static Content

51. Akamai Technologies Inc. is used as a content delivery network (CDN) services provider for static content. The location of the data corresponds to the Webex data centre assignment of the Customer, which is in the case of the CJEU is Frankfurt, Germany, with back-up in Amsterdam. Data sent to Akamai would, therefore, be located initially in the EU.

52. To create logs used – for example for troubleshooting – Akamai may process the IP address, browser and geographic region of a user. Those logs may, however, be transferred to the United States.

4) WebEx signalling service

53. Amazon Web Services, Inc. (AWS) is used to host the WebEx signalling service that processes real-time meeting lifecycle information, namely meeting participant UUIDs as well as meeting start and end times.

54. The processing by AWS can be located in the United States, the United Kingdom, Brazil, Australia, Japan, Singapore or the EU. The data is deleted within 15 days of the meeting.

55. As part of Cisco's Webex Data Residency program, AWS has taken measures that data for those Webex Meetings customers provisioned within the EU would be processed within the EU.

56. Furthermore, Cisco's encryption methods preclude AWS from having access to this raw data in the clear.

5) WebEx media nodes

57. AWS cloud infrastructure is also used to host Webex media nodes that may process real-time meeting data such as VoIP, video and high frame rate sharing data.

58. To provide Global Distributed Meetings functionality within Webex, where users are able to connect to the closest media node for better performance, processing by AWS can be located in the United States, the United Kingdom, Brazil, Australia, Japan, Singapore or the EU.

59. The data is not stored by AWS and transferred data is encrypted during transit. Cisco's encryption methods preclude AWS from having access to this raw data in the clear.

B. Use of TAC Support

60. The use of TAC support leads to the processing of TAC Support Information and the Customer case attachment(s), which may also include personal data. In order to provide support, Cisco can also access and process User Information as well as Host and Usage Information.

61. The personal data contained in the Customer case attachment(s) is under the control of the customer that opens the request for support. The customer can decide whether it is appropriate to include personal data.

62. The information used to provide support can also include the UUID of users for scheduled meetings that do not involve the use of Webex, such as meetings with physical presence or other appointments. This is the case when the Hybrid Calendar Service is used and information on all meetings in the Outlook Calendar is transmitted to Cisco. The information with regard to meetings without Webex is, however, end-to-end encrypted and not accessible for Cisco, except for the UUID which remains accessible in the logs of the service. These logs can be used in order to provide support.

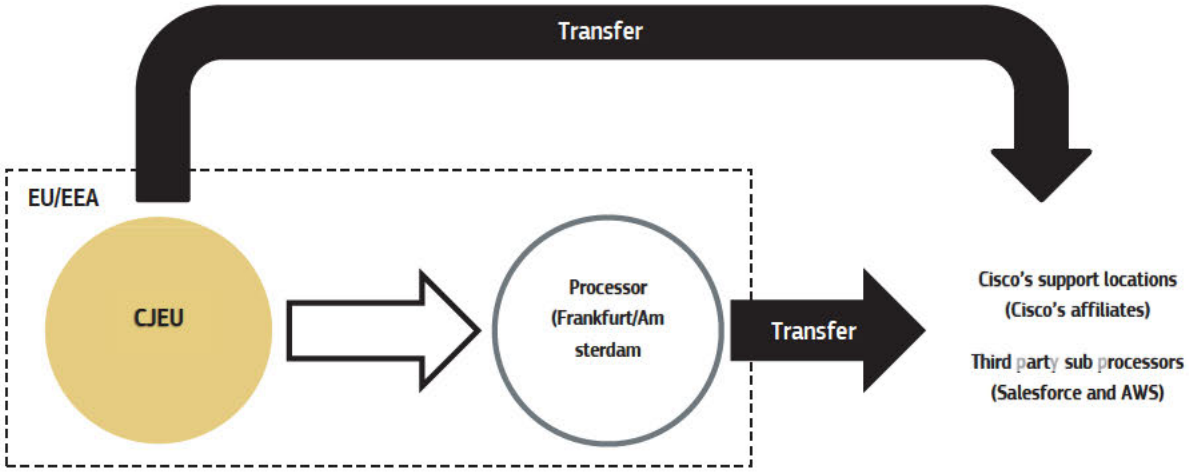
63. The TAC support information and Customer case attachment(s) are transferred in all situations to the United States, and more specifically to Salesforce (for TAC support information) and Amazon Web Services (for Customer case attachments). TAC Support Information and Customer case attachments are, however, only accessed by Cisco. No personnel from third-party service providers have access to this data.

64. Customer case attachments are, furthermore, considered customer data and are encrypted both in transit and at rest by Cisco.

65. The TAC support information and Customer case attachments, as well as User Information and Host and Usage Information required for a TAC case, can be accessed remotely and can, therefore, be transferred. This is because Cisco's TAC support follows a "follow the sun" approach, whereby if an EU customer contacts TAC during non-business hours within the European time zones (GMT+1/+2), the TAC case may be handled by support staff outside of the EU. A transfer can accordingly take place to the United States, the United Kingdom, India or Jordan.

66. To limit such transfers, CJEU customers should call Cisco TAC support during the standard EU business hours, in which case their case is more likely handled by TAC support within the EU. CJEU users can also minimise personal data transfers by minimising the personal data reflected in the case attachments.

67. The data flow for TAC support can therefore be summarised as such:



C. Countries of destination

68. In conclusion, a transfer of personal data can take place from the processor in the EU to the following third countries: the United States, United Kingdom, Brazil, Australia, Japan, Singapore, India or Jordan.

IV. TRANSFER TOOLS

A. Adequacy decision

69. A transfer of personal data to the United Kingdom or Japan takes place on the basis of the following adequacy decisions in which the European Commission has concluded that these countries ensure an adequate level of protection:

– Commission Implementing Decision (EU) 2021/1772 of 28 June 2021 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by the United Kingdom (notified under document C(2021)4800) (OJ 2021, L 360, p. 1); and

– Commission Implementing Decision (EU) 2019/419 of 23 January 2019 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by Japan under the Act on the Protection of Personal Information (OJ 2019, L 76, p. 1).

70. The transfers of personal data to these countries do, therefore, not pose a risk for the data subjects and no further supplementary measures are needed, as long as the Commission does not establish that these countries no longer ensure an adequate level of protection.

B. Appropriate safeguards

71. Further transfers of personal data can also take place to recipients in the United States, Brazil, Australia, Singapore, India or Jordan.

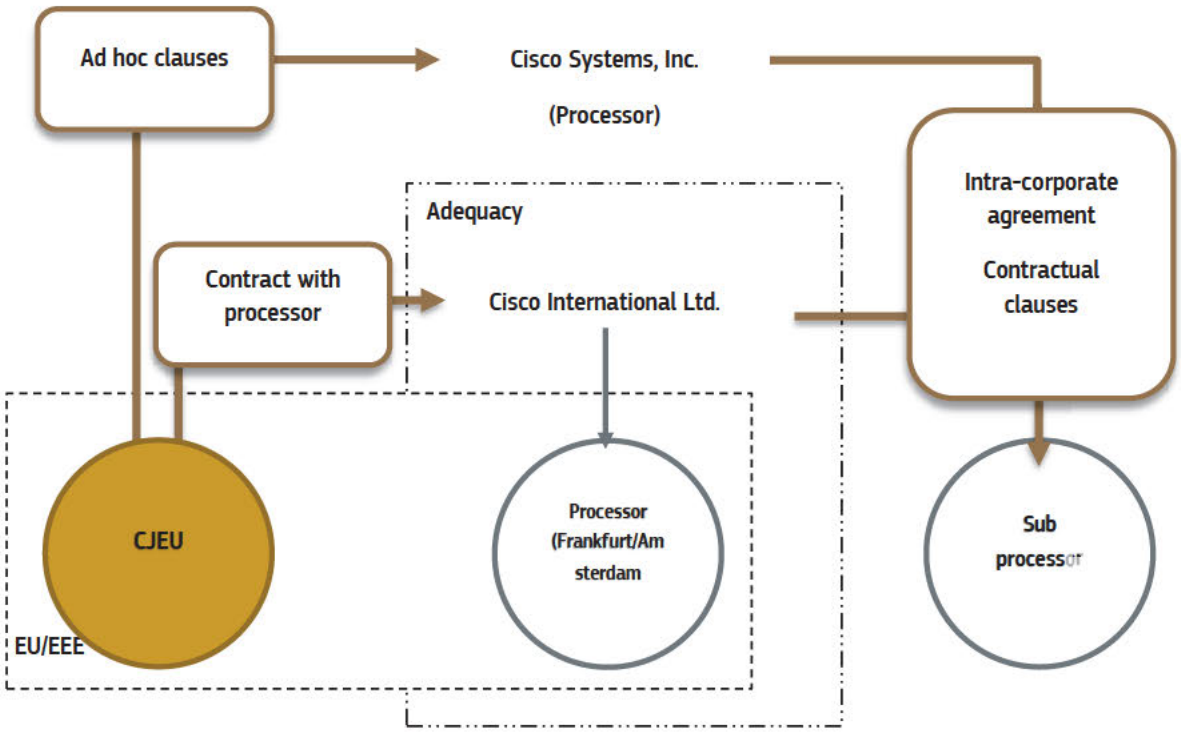
72. The transfers from the CJEU to Cisco Systems, Inc., as a processor and data importer, take place on the basis of ad hoc clauses authorised on the basis of Article 48(3)(a) of Regulation (EU) 2018/1725[1].

73. A temporary authorisation of ad hoc clauses has been provided by the decision of the EDPS. In order to comply with the requirement of the EDPS, a new set of ad hoc clauses is prepared. The data transfer impact analysis is based on these new clauses, which will be submitted for authorisation by the EDPS.

74. Cisco International Ltd. accepts that the ad hoc clauses are an integral part of the Agreement and its Amendment concluded between Cisco International Ltd. and the CJEU. In this manner, Cisco International Ltd. endorses towards the CJEU all obligations taken by Cisco Systems, Inc. under these ad hoc clauses.

[1] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ 2018, L 295, p. 39).

75. The use of appropriate safeguards based on different contractual clauses and the passing on of contractual obligations can be presented like this:



76. In accordance with the requirement of the EDPS in its decision, the standard contractual clauses for transfers under the GDPR adopted by the Commission ("the SCCs") for transfers are used for the drafting of the new ad hoc contractual clauses.

77. The SCCs have been adapted to reflect the situation of an EU institution on the following formal points:

- Where appropriate, a reference to regulation (EU) 2018/1725 and the relevant articles has been included. The EDPS has also been identified as supervising authority.
- The exclusive jurisdiction of the CJEU is taken into account with regard to cases brought by a data subject against the institution.

78. The further additional measures adopted in order to provide appropriate safeguards are discussed below.

C. Effectiveness and remaining risks

79. The access by public authorities of a third country to the personal data transferred cannot be entirely excluded for transfers to countries not covered by an adequacy decision.

80. In accordance with the decision of the EDPS, the CJEU should also consider all examples of supplementary measures in Annexe 2 of the EDPB Recommendations 01/2020, to identify which supplementary measures that would be necessary and appropriate to implement for transfers in the Court's use of Cisco Webex Meeting and related services.

81. The CJEU has, therefore, examined and adopted supplementary measures, as described below. These measures also include measures taken over from the SCCs that reflect the requirements of the EDPS as stated in its decision.

V. SUPPLEMENTARY MEASURES

A. Technical measures

1) ENCRYPTION OF DATA TO PROTECT IT FROM ACCESS BY THE PUBLIC AUTHORITIES OF THE THIRD COUNTRY OF THE IMPORTER WHEN IT TRANSITS BETWEEN THE EXPORTER AND ITS IMPORTER

82. This measure corresponds to Use Case 3 in Annexe 2 of the EDPB Recommendations 01/2020.

83. Cisco encrypts personal data associated with the use of Webex in transit and at rest.

84. All communications between cloud registered Webex Apps, Webex Room devices and Webex services occur over encrypted channels. Webex uses the TLS protocol with version 1.2 or later with high strength cipher suites for signalling.

85. After a session is established over TLS, all media streams (audio VoIP, video, screen share, and document share) are encrypted.

86. Encrypted media can be transported over UDP, TCP, or TLS. Cisco prefers and strongly recommends UDP as the transport protocol for WebEx voice and video media streams. This is because TCP and TLS are connection orientated transport protocols, designed to reliably deliver correctly ordered data to upper-layer protocols. Using TCP or TLS, the sender will retransmit lost packets until they are acknowledged, and the receiver will buffer the packet stream until the lost packets are recovered. For media streams over TCP or TLS, this behaviour manifests itself as increased latency/jitter, which in turn affects the media quality experienced by the call's participants.

87. Technical details about Cisco's encryption methods, including for example ciphers, are found in Cisco's publicly available Privacy Data Sheets, located on the Cisco Trust Portal at the following link: https://trustportal.cisco.com/c/r/ctp/trust-portal.html#/.

88. As of this writing, media packets are encrypted using either AES 256 or AES 128 based ciphers. The Webex App and Webex Room devices use AES-256-GCM to encrypt media; these media encryption keys are exchanged over TLS-secured signalling channels. SIP and H323 devices that support media encryption with SRTP can use AES-256-GCM, AES-128-GCM, or AES-CM-128-HMAC-SHA1 (AES-256-GCM is the WebEx preferred media encryption cipher).

89. Additionally, Cisco encrypts data associated with TAC support at least in transit, and for case attachments both in transit and at rest, in order to secure personal data from accidental loss and unauthorised access, use, alteration, and disclosure.

90. Details about Cisco's encryption methods can be found in the publicly available TAC Privacy Data Sheet found at the following link: https://trustportal.cisco.com/c/r/ctp/trust-portal.html#/1552559092863136.

91. These measures allow for protection of all data in transit.

2) WEBEX ZERO TRUST SECURITY END-TO-END ENCRYPTION

92. The use of Webex Zero Trust Security End-to-End encryption ensures that Cisco cannot decipher the media streams of a meeting, but instead only relays it forward to participants as received. The exchange of keys between participants to the videoconference is made without Cisco being able to access these keys[2].

93. The use of WebEx Zero Trust Security End-to-End encryption is enforced when a user at the CJEU organises a videoconference.

[2] For more information, see the Zero-Trust Security for Webex Whitepaper (https://www.cisco.com/c/en/us/solutions/collateral/collaboration/white-paper-c11-744553.html).

94. As a consequence, cloud-provided features like transcription or recordings cannot be used in this type of meeting, because the media stream never reaches the cloud. However, User Information and Host and Usage information – i.e. metadata – is sent to the cloud and can, therefore, be the object of a transfer of personal data.

95. This measure allows, therefore, for a protection of User-Generated information.

96. In situations where the use of Webex Zero Trust Security End-to-End encryption is technically not possible, the CJEU will either use alternative solutions (such as Cisco Meeting Server) or will evaluate the level of protection required for the specific meeting (for example public or semi-public meeting).

97. This might be necessary in situations where the meeting needs to be recorded or where an external user cannot use Webex Zero Trust Security End-to-End encryption. This last situation can be due to the infrastructure in an external meeting room used for the videoconference or because the user wants to call in by phone or because of the use of a Linux client. The CJEU has taken measures to limit these situations by equipping its own meeting rooms with a compatible infrastructure and by blocking the possibility to call in by phone (use of VoIP Only). When necessary, the requirements for the proper use of Webex Zero Trust Security End-to-End encryption will also be communicated by the CJEU to external users before the meeting.

98. Cisco provided information about Webex Zero Trust Security End-to-End encryption through its publicly available Webex Meetings Privacy Data Sheet, found at the Cisco Trust Portal linked above.

99. In accordance with internal CJEU policies and setup, the only services that could organise a videoconference without Webex Zero Trust Security End-to-End encryption are the Training and Development unit (in order to record certain training sessions) or the Information Technology Directorate of the CJEU (in order to set up videoconferences for users where WebEx Zero Trust Security End-to-End encryption is not possible).

3) MEDIA NODE LOCATED IN THE EU

100. Global Distributed Meetings ("GDM") enables a meeting to be distributed to multiple servers running in different data centres. In order to limit the transfer of personal data, the CJEU imposes the use of media nodes located within the EU/EEA through the deactivation of GDM.

101. Webex media nodes are controlled by Cisco, meaning that Cisco manages the access and provides the services. AWS, as a sub processor, provides the infrastructure offering virtual servers and cloud storage.

102. The infrastructure of AWS is used to process real-time meeting data such as VoIP, video and high frame rate sharing data.

103. The use of media nodes located solely within the EU/EEA avoids a transfer of personal data to media nodes located outside the EU/EEA.

104. This measure contributes, therefore, to the fulfilment of the requirement of the EDPS according to which no transfers of personal data, including by remote access, occur due to Cisco's reliance on data centre services provided by AWS.

105. It, furthermore, allows for the protection of User-generated information.

106. The data processed by media nodes provided by AWS would, however, be encrypted and, therefore, not be accessible to AWS. The encryption keys would either be in the possession of Cisco or, in case WebEx Zero Trust Security End-to-End encryption is used, in the possession of the users. This encryption alone and the control of Cisco over the media node could, therefore, be considered to be a sufficient measure to prevent an access to personal data by AWS.

B. Additional contractual measures

1) Docking clause

107. The ad hoc clauses contain a docking clause, which allows for other sub-processors to adhere to them as well. This clause is taken over from the SCCs and adapted to the contract concluded between the CJEU and Cisco.

108. It allows for other recipients to whom data will be transferred in the CJEU's use of Cisco Webex Meeting and related services to adhere to the new ad hoc contractual clauses concluded by the Court and the measures foreseen to assure the protection of personal data. This clause therefore complies with the requirement of the EDPS with regard to the possibility for other recipients to whom data will be transferred in the Court's use of Cisco Webex Meeting and related services to adhere to the new ad hoc contractual clauses concluded by the Court.

2) Transparency and obligations to take specific actions

109. The contract contains a clause with regard to the obligation of Cisco to inform the CJEU of any legally binding request for disclosure of the personal data processed or, if this is not possible, the obligation to challenge the request by exhausting all potentially viable remedies.

110. The ad hoc clauses also contain clauses with regard to local laws and practices affecting compliance with the clauses as well as with regard to the obligations of the data importer in case of access by public authorities. The ad hoc contractual clauses bind Cisco Systems, Inc. directly.

111. These clauses are adopted taking into account the requirement of the EDPS with regard to the transparency obligations of Cisco.

112. Regarding country-specific information on local law compliance, both Webex and TAC are certified for ISO 27001 (which has a requirement for the identification of applicable legislation & contractual requirements (control 18.1.1)).

3) No back door policy

113. The contract provides for a specific clause that Cisco would not create programming functions that could be used to access, transmit or send personal data without the authorisation of the CJEU.

114. Cisco, furthermore, certifies that it would not create or maintain programming functions designed to facilitate access by a public authority to personal data.

115. This obligation is added to the contract with Cisco International Limited and is part of the additional commitments added to the ad hoc contractual clauses.

116. This clause is added to respond to the requirement of the EDPS with regard to the "no back door" policy.

4) Access to data by Cisco

117. The contract provides for a specific clause that Cisco does not access the data of the CJEU by default, i.e. without a support request. In order to provide support, Cisco will work with the data provided by the CJEU and has agreed to seek the data exporter's explicit authorisation to access additional data required for support.

118. This obligation is added to the contract with Cisco International Limited and is part of the additional commitments added to the ad hoc contractual clauses.

119. This clause is added to respond to the requirement of the EDPS with regard to the access to the personal data.

5) Specific training procedures

120. The contract provides for a specific clause that Cisco will ensure that specific training policies for personnel in charge of managing requests for access to personal data from public authorities are in place.

121. This obligation is added to the contract with Cisco International Limited and is part of the additional commitments added to the ad hoc contractual clauses.

122. This clause is added to respond to the requirement of the EDPS with regard to the specific training policies and procedures.

6) Obligation to pass on essentially equivalent obligations to further processors

123. A specific obligation is added to the contract and the ad hoc clauses with regard to the use of sub-processors and onward transfers.

124. Onward transfers of personal data occur on the bases of contractual clauses concluded between the different Cisco entities as part of their intra-corporate agreement or on the basis of contractual clauses concluded between Cisco (as processor) and its third-party sub-processors. These clauses should be based on the standard contractual clauses for the transfer of personal data to third countries, adopted by the Commission on the basis of Article 46(2)(c) of Regulation (EU) 2016/679 and have to respect the technical and organisational measures foreseen in the contract between the CJEU and the processor.

125. These contractual obligations prevail over any other contractual obligation between the data importer and the sub processor or, as the case may be, between a sub processor and a sub processor.

126. These clauses are added to respond to the requirement of the EDPS with regard to the effectiveness of the obligations with regard to the processing of personal data.

C. Organisational measures

1) Customer, User, Or User Administrator Actions

127. The CJEU has taken measures to limit or avoid transfers of personal data outside of the EU/EEA following action from users or user administrators. These measures are the following:

a) The users of the CJEU do not need to register themselves on any Cisco platform or a Cisco service in order to use Webex. External users are also not required to perform such a registration.

b) The ordering information for the use of Webex by the user of the CJEU is handled in the contract. No further business contact information is required for the use of Webex by the CJEU.

c) Specific collaborations tools included in Webex such as Webex Calling or Webex Messaging are not used by the CJEU. Furthermore, the CJEU will use only media nodes located in the EU (see Media node located in the EU).

d) The CJEU will ensure that users do not directly open a support case (see Opening of a support case).

e) Optional functionalities that might necessitate a transfer of personal data without appropriate safeguards are blocked by the CJEU when the CJEU is aware of the functionality and the functionality can be blocked.

Such functionalities are 3rd party telephony, 3rd party applications via Webex App hub or third-party application stores (Slido).

f) "Push" notifications can be configured locally on Mobile Devices by the user and can, therefore, not be entirely controlled by the CJEU. The CJEU does, however, impose that, in principle, only professional devices are used for work related communications.

128. This measure allows, therefore, for a protection of User-Generated Information as well as User Information and Host and Usage information.

2) Alternative solutions: Cisco Meeting Server and streaming service

129. The CJEU does not only use Webex for organising videoconferences.

130. For meetings or conferences requiring a higher level of security, the CJEU will use its Cisco Meeting Server, where all data is processed on premises.

131. For events that require the ability for a large number of people to follow the event remotely, without active participation, the CJEU can have recourse to the streaming service provided by another provider.

132. These solutions allow, in particular, to limit the processing and transfer of personal data from external participants who will not be required to log in to Cisco Webex in order to attend a meeting or event organised by the CJEU. Users of the CJEU will also not provide their personal data linked to their participation to that specific meeting.

133. This measure allows, therefore, for a protection of User-Generated Information as well as User Information and Host and Usage information.

3) PRIVATE MEETING

134. The use of the regular Webex Cloud services for the processing of User-Generated information is limited to videoconferences involving external participants. Videoconferences among users of the CJEU (either in the office or teleworking with the material provided by the CJEU) will be processed on premises with the use of Private Meeting and Cisco Video Mesh.

135. As a consequence, cloud-provided features like transcription, or recordings cannot be used in this type of meeting because the media stream never reaches the cloud. However, User Information and Host and Usage information is sent to the cloud and can, therefore, be the object of a transfer of personal data.

136. This measure allows, therefore, for a protection of User-Generated information.

4) MEASURES ENABLED BY CJEU TO LIMIT PERSONAL DATA TRANSMISSION

137. The CJEU has undertaken certain measures and implemented certain policies to limit transfers of personal data falling under the categories of User Information and Host and Usage Information. Notably, this may limit the features and functionalities of Webex, and in some cases may affect performance.

138. Those are described below:

Personal data	Measure
User Information	
Phone Number Mailing Address Password User Information Included in Your Directory	The CJEU uses an identity provider (F5) to identify the users of the CJEU and transmit their data to Cisco through a SAML protocol. The personal data transmitted is restricted to the name and e-mail address.
Avatar	An avatar can be chosen by the user. If the user does not use an avatar, no avatar is processed.
Host and Usage information	
IP Address (for internal users) IP Addresses Along the Network Path (for internal users)	Internal users – including users who are connected remotely – will use the IP address of the CJEU, which does not allow for the identification of a user by Cisco or its sub processors.
Call attendee information, including e-mail addresses, username, phone numbers, room device information	A user name for external users will only be requested in a manner allowing for the identification of a physical person when this is required for the proper conduct of the meeting or event organised. In other cases, an external user can use a pseudonym as user name. The CJEU will not require external users to provide the e-mail addresses, phone numbers or room device information when joining a meeting. All meetings are conducted with VOIP only, which avoids transmission of phone numbers to conduct a Webex meeting.

5) OPENING OF A SUPPORT CASE

139. The CJEU will ensure that users do not directly open a support case. When support is needed, the user at the CJEU will have to contact the internal helpdesk, which will then, if required, contact Cisco. This measure will limit the TAC Support Information to the persons designated to open a possible support case with Cisco and will offer the CJEU better control on the content of the Customer Case Attachment(s).

140. Furthermore, as the CJEU will open a support case during EU business hours, these support cases will initially be dealt with by Cisco entities within the EU.

141. The CJEU can also request the deletion of personal data retained by TAC support by submitting a request to Cisco via the Privacy Portal.

6) INTERNAL POLICIES AND GUIDELINES FROM THE CJEU

142. Currently, not all users at the CJEU can organise themselves meetings in Webex. In order to offer this function to all users, the CJEU will adopt internal policies that will cover the following subjects:

- instructions and rules on the choice of tools for videoconferencing;
- Instructions and rules on the potential use of private devices for videoconferencing;
- instructions and rules on the requests for support by staff and by the internal helpdesk, including a consultation of the DPO and requests to delete personal data after the closure of the support case;
- updated documentation and information notice to be provided internally and externally, including the technical requirements for the use of Webex zero trust E2EE.

VI. CONCLUSION ON THE RISKS FOR DATA SUBJECTS

A. Overview

143. The different remaining transfers and measures taken to assure appropriate safeguards are summarised in the following table:

Service	Personal data transferred	Country of destination	Measures
Webex Meetings & Webex App	User Information Host & Usage Information User-Generated Information	In some circumstances based on customer, user, or user admin actions, could be transferred to the United States	Functions disabled by the CJEU
Step-by-step tour and guidance	Unique User ID User region	United States	EU Data residency program Function disabled by the CJEU
Extended capacity for WebEx Meetings	Name Unique User ID User region	United States Australia	EU Data residency program Function disabled by the CJEU
Static content	IP address Browser User region	United States	EU Data residency program Contractual clauses between Cisco and sub-processor
WebEx signalling service	Meeting participant Unique User ID Meetings start and end times	United States Brazil Australia Singapore	EU Data residency program Contractual clauses between Cisco and sub-processor
		United Kingdom Japan	Adequacy decision
WebEx media nodes	VoIP Video High frame rate sharing data	United States Brazil Australia Singapore	Media node in the EU Encryption by Cisco End-to-end encryption

		United Kingdom Japan	Adequacy decision
TAC Support	Customer case attachment User Information Host and Usage Information	United States India Jordan	Contractual clauses between Cisco and sub-processor Encryption by Cisco
		United Kingdom	Adequacy decision

B. Conclusion

1) User-generated information

144. The CJEU has taken specific measures to limit the processing of User-Generated Information in the Cloud by the use of Private Meeting. Furthermore, alternative tools can be used when required, such as Cisco Meeting Server. These measures limit the amount of personal data transferred and exclude transfer of sensitive data.

145. When a videoconference uses the cloud infrastructure, the content of the conference is protected by end-to-end encryption, in a way that Cisco does not have access.

146. In the light of these elements, the protection of the personal data that falls in the category User-Generated information is effective.

2) User information and Host and usage information

147. The CJEU has taken several measures to ensure an effective protection of User Information as well as Host and Usage information. Specifically, the situations in which this data is transferred are restricted through their storage in the EU/EEA, the limitation of functions that would require a transfer and the conditions for access to the data.

148. Where possible, measures have also been taken to limit the data provided to what is strictly necessary. This concerns specifically external users that will be required to provide only a user name. In order to protect the personal data of external users, alternative tools can be used when required, such as Cisco Meeting Server.

149. A further restriction in the functionalities or limits to access the data in order to avoid a transfer of personal data does not appear to be feasible and would hamper to the provision of the service, and in particular the support in the use of the service.

150. In the situations where a transfer does occur, in particular through remote access, supplementary safeguards are offered by the contract and through organisational measures. These measures are based on the recommendations of the EDPS in its decision as well as further internal measures adopted by the CJEU.

151. The measures adopted would appear to offer effective protection of the personal data concerned.

3) Data subject rights and effective legal remedies

152. The data subject rights and legal remedies added in the ad hoc contractual clauses are taken over from the SCCs. These clauses foresee in third party beneficiary rights, the exercise of data subject rights under Regulation (EU) 2018/1725, a redress mechanism, notification obligations in case of access by public authorities, the obligation to review the legality of such a request and the obligation to challenge unlawful requests.

153. These rights and remedies, in the light of the measures taken to limit the transfer of personal data, offer an appropriate level of protection of personal data.

Taken together, the adopted measures offer appropriate safeguards to assure the protection of personal data. These measures will be reviewed in light of any change of circumstances (factual, regulatory or technical), and at least once per year.

Further measures could include a modification of the agreement by a written amendment accepted by both parties, the termination of the agreement and/or a halt to any transfers.

Mr Wojciech Rafał Wiewiórowski
European Data Protection Supervisor
Rue Wiertz 60
1047 Brussels
BELGIUM

edps@edps.europa.eu

Luxembourg, 1 September 2022

BY E-MAIL

Your reference: C 2021-0255

Request for authorisation in accordance with Article 48(3)(a) of Regulation (EU) 2018/1725

Dear Sir,

The European data protection Supervisor ("EDPS") adopted its decision to temporarily authorise the use of ad hoc contractual clauses between the Court of Justice of the EU ("CJEU") and Cisco for transfers of personal data in the CJEU's use of Cisco Webex and related services on August 31, 2021 (case 2021-0255).

According to the decision, the CJEU was required to remedy the compliance issues identified to ensure an essentially equivalent level of protection within one year from the date of this decision.

The CJEU has, therefore, requested Cisco to modify their global product to comply with the EU legal framework and negotiated an amendment to the contract with Cisco International Limited as well as a new set of ad hoc contractual clauses for the transfer of personal data between the CJEU and Cisco Systems, Inc. The draft amendment and the ad hoc contractual clauses are attached as annex I.

In compliance with the requirements of the decision, the CJEU as also carried out a transfer impact assessment, with the assistance of Cisco. The transfer impact assessment is attached as annex II.

In accordance with Article 48(3)(a) of Regulation (EU) 2018/1725 and the decision, the CJEU request a renewal of the authorisation for the use of ad hoc contractual clauses between the CJEU and Cisco Systems Inc. as a means for adducing appropriate safeguards in the context of transfers of personal data in the Court's use of Cisco Webex and related services.

In order to comply with the requirement from the decision, the following measures have been foreseen:

- The remaining transfers of personal data and **data flows**, taking into account the use of Cisco's cloud services by the CJEU, are described in the **transfer impact assessment**. The assessment takes into account the **storage of personal data in the EU** for the use of Cisco Webex Services and identifies the remaining transfers and accompanying measures, including those resulting from the use of sub processors (see conditions 1, 2 and 3).

- The **new set of ad hoc contractual clauses** (Exhibit A to the amendment) are based on the model of the new standard contractual clauses for transfers under the GDPR adopted by the Commission. The new ad hoc contractual clauses will be **signed by Cisco Systems, Inc. as an importer, while Cisco International Limited accepts that the resulting obligations are an integral part of the Agreement and its Amendment** (Article 1(4)(d), second paragraph of the amendment) concluded between the CJEU and Cisco International Limited) (see conditions 4 and 5).

- The **ad hoc Standard Contractual Clauses prevail over any other contractual obligation** (clause 9(f) of the ad hoc contractual clauses) between the data importer and the sub-processor or, as the case may be, between a sub-processor and a sub-processor. This includes the obligations with regard to local laws and practices in clause 14 of the ad hoc contractual clauses and its obligations with regard to **disclosure requests**[1], which are taken over from the new standard contractual clauses for transfers under the GDPR adopted by the Commission (see conditions 6 and 9).

[1] Article 1(4)(c), fourteenth paragraph of the amendment also contains obligations with regard to disclosure requests towards Cisco International Limited.

- The **annexes to the ad hoc contractual clauses** (annexes 1a and 1b to exhibit A of the amendment) describe the remaining transfers of personal data and applicable measures for the use of Webex and TAC support, as these are the services used by the CJEU (see condition 7).

- The obligations from the ad hoc contractual clauses have to be **passed on to other recipients of personal data** based on the general obligation to pass on the essentially equivalent obligations to those referred to in Article 1(4) of the amendment (Article 1(4)(c), eighteenth paragraph of the amendment) as well as, in case of an onward transfer by Cisco Systems Inc., the obligation to assure technical and organisational measures that, at least, reach the same level of security as those foreseen in Exhibit C to the amendment (clause 9(f) and (g) of the ad hoc contractual clauses). The role and the processing of transferred data by sub processors listed in Exhibit B have been assessed in the Transfer Impact Assessment (see condition 8).

- Specific clauses have been added in the amendment and as additional commitments in annexes 1a and 1b to the ad hoc clauses with regard to a **"no back door policy"** (Article 1(4)(c), sixteenth paragraph of the amendment and Title C of annexes 1a and 1b to exhibit A of the amendment), the **access to personal data** (Article 1(4)(c), twentieth paragraph of the amendment and Title C of annexes 1a and 1b to exhibit A of the amendment) and **specific training procedures** (Article 1(4)(e) of the amendment and Title C of annexes 1a and 1b to exhibit A of the amendment) (see conditions 10, 13 and 14)

- The **use of End to end encryption** is described in annexes 1a and 1b to exhibit A of the amendment (see condition 11).

- The **technical and organisational measures** used are described in Cisco's Information Security Exhibit, in exhibit C to the amendment (see condition 12).

This draft amendment also takes into account the Webex Data Residency for Webex Meetings customers located in the EU, implemented by Cisco in the course of the discussions between Cisco and the CJEU. Indeed, Cisco released the **new version of their global product,** in which the data transfers to US for billing and analytics were stopped, before end July 2022. Webex data residency provides Webex Meetings customer user administrators the ability to choose where their organisation's data is stored, in particular personal data processed by Webex Meetings. Data associated with the CJEU has thus been migrated to the EU.

I remain at your disposal to answer any further questions in this regard.

Yours sincerely,

[signed]

[redacted]
Court of Justice of the European Union

Annexes:

I. Draft amendment to the contract with Cisco International Limited, including ad hoc contractual clauses for the transfer of personal data between the CJEU and Cisco Systems, Inc.
II. Data transfer impact assessment for the use of Cisco Webex by the Court of Justice of the European Union