From:	DataProtectionOfficer <DataProtectionOfficer@curia.europa.eu>
To:	European Data Protection Supervisor <EDPS@edps.europa.eu>
CC:	[redacted]
Sent at:	28/02/22 08:39:35
Subject:	Case 2021-0255 - Intermediate compliance report on the implementation of the conditions set for the renewal of the authorisation for the use of ad hoc contractual clauses

Dear Madam,
Dear Sir,

Please find enclosed a letter for the attention of the Data protection supervisor with regard to the Court's intermediate compliance report on the implementation of the conditions set for the renewal of the authorisation for the use of ad hoc contractual clauses between the Court and Cisco.

Best regards,

[redacted]

COURT OF JUSTICE
OF THE EUROPEAN UNION

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

[redacted]

INTERMEDIATE COMPLIANCE REPORT ON THE IMPLEMENTATION OF THE CONDITIONS SET FOR THE RENEWAL OF THE AUTHORISATION FOR THE USE OF AD HOC CONTRACTUAL CLAUSES FOR THE TRANSFER OF PERSONAL DATA

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") 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. According to the decision, the CJEU is to provide to the EDPS an intermediate compliance report demonstrating steps taken to implement the conditions set for the renewal of the authorisation. This report shall include information on progress on the commitments undertaken by the CJEU and those undertaken by Cisco.

4. The present report gives an overview of the ongoing negotiations with Cisco and the steps taken in order to comply with each condition set by the EDPS.

NEGOTIATIONS WITH CISCO

5. After internal discussions and after having informed the EDPS, the CJEU has communicated the decision of the EDPS to Cisco on 15 October 2021. The decision was then also published by the EDPS on its website.

6. Discussions with Cisco took place on 25 November 2021, after which Cisco provided a document summarising its actions on the specific recommendations. This document was updated by Cisco on 25 January 2022 and complemented with a proposal to amend the contract.

7. The CJEU has provided to Cisco its remaining questions in order to clarify certain points and its own proposal for the amendment of the contract.

8. The present report gives an overview of the proposals to modify the contract in view of each of the conditions set by the EDPS. All information given is therefore still subject to negotiations between the parties and can evolve further.

MEASURES TAKEN

9. At this stage, the CJEU and Cisco are working on the clarification of the data flows and the necessary modifications to the contract.

10. Cisco also continues its work on the commitment to store all "User Information" and "Host and Usage Information" within the EU. Currently, it is envisaged that this will be accomplished by July 2022. The deadline set in the initial contract has therefore been extended a first time. The CJEU continues to follow up on this issue and will take this into account in the final proposal to amend the contract.

11. It is also envisaged to modify the structure of the contract with, on the one hand, a part covering the obligations of Cisco International Limited as processor and, on the other, a part covering the specific obligations with regard to transfers of personal data to a third country that is not covered by an adequacy decision and the related ad hoc contractual clauses that will be binding on Cisco Systems, Inc., Cisco International Limited and any sub-processor processing such data.

12. Hereinafter, the present report gives further explanations on the current stage of implementation of each of the 14 conditions set by the EDPS in the decision.

1. Data flows

13. The EDPS wishes that the CJEU clearly 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.

14. As a first step, the CJEU has clarified the setup of Cisco Webex that will be used.

15. At the same time, Cisco reviewed its data privacy sheets in order to provide a more comprehensive information. This information will be included in the contractual documents as an exhibit to the contract.

16. The CJEU has nevertheless asked several clarifications to Cisco with regard to the data flows, in order to leave out any ambiguities.

17. The questions asked concern the following points:

The exhaustive identification of the services covered and their corresponding data flows.

18. The description of data flows covers the use of Webex Meetings and the use of TAC support services.

19. The question has also arisen – and is being dealt with – whether any other services required the processing of personal data by Cisco and whether certain data would not be processed when using specific setups. This is specifically relevant for the use of Webex app, the use of Webex Meetings with Zero Trust Security End-to-End encryption, the use of Cisco Private Meetings and the Cisco Meeting Server.

20. Not all of these data flows will include, however, a transfer of personal data. Once the data flows are clarified, the personal data that will be the object of a transfer to a country not covered by an adequacy decision will be identified and will be included in the ad hoc contractual clauses and taken into account in the transfer impact assessment.

21. The main points for which the CJEU has requested further clarifications can be summarised as follows:

The definition of the types of data used

22. Cisco was invited to provide a description of certain types of personal data used or to complete any description that is not exhaustive in order to avoid terms like “such as” or “limited Host & usage Information”.

23. With regard to the customer support, Cisco is asked to clarify whether the “Customer Case Attachments” is entirely under the control of the client, or whether this information can be complemented by other elements by Cisco.

24. The same terminology should also be used throughout the description of the data flows.

Changes to existing data flows and remaining transfers

25. Cisco has been asked to clarify the data flows once that "User Information" and "Host and Usage Information" will remain in the EU. This clarification should also take into account any situation of remote access from a third country and its potential use to provide support.

26. All situations where a transfer of personal data might still take place should also be clarified.

Role of sub-processors

27. The processing by certain sub-processors needs further clarification, especially with regard to their role and the possibility to exclude the use of their services by other measures.

2. Data storage

28. The EDPS wishes that all personal data in the CJEU's use of Cisco Webex services, i.e. user information, host and usage information, user-generated information, billing data and analytics data, are stored/reside in the EU, in accordance with the contract concluded between the CJEU and Cisco. In particular, Webex meeting and connection data (including personal data) in the CJEU's use of Cisco Webex services (whether on premises or cloud-based) should be stored/reside in the EU and for cloud-based Cisco Webex services no transfers of that data, including by remote access, should occur due to Cisco's reliance on data center services provided by AWS.

29. The fulfilment of this requirement is dependent on the progress of Cisco to complete its EU residency programme. According to the latest information provided by Cisco, the "User Information" and "Host and Usage Information" will remain in Frankfurt after July 2022.

30. If it is confirmed that that personal data will no longer be transferred, including by remote access, to a country not covered by an adequacy decision for the use of Webex, this processing operation will no longer require the use of ad hoc clauses.

3. Transfer impact assessment

31. The EDPS wishes that in relation to all other types of personal data, namely 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, the CJEU carries out a transfer impact assessment, 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 standard contractual clauses for transfers under the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC ("GDPR") as adapted to the 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 ("the Regulation"). The CJEU should consider all examples of supplementary measures in Annex 2 of the EDPB Recommendations 01/2020, to identify which supplementary measures would be necessary and appropriate to implement for transfers in the CJEU's use of Cisco Webex Meeting and related services.

32. The work on the transfer impact assessment will be finalised once the data flows are fully clarified.

33. Nevertheless, any identified gaps in the level of protection provided are already taken into account for the adoption of further measures to assure an appropriate level of protection of any personal data that is transferred outside the EU/EEA.

34. The assessment shall also include the elements required under clause 14(b) of the ad hoc contractual clauses that provide that due account is taken 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.

4. New ad hoc contractual clauses

35. The EDPS wishes that new ad hoc contractual clauses are concluded based on the model of the new standard contractual clauses for transfers under the GDPR adopted by the Commission1 ("the SCCs") as adapted to the Regulation, include updated relevant clauses in the main body of the contract and provide for effective contractual safeguards and commitments on technical and organisational measures.

36. Module two of the SCCs for transfers "controller to processor" are used for the adoption of a new set of ad hoc contractual clauses. The current proposal for the ad hoc contractual clauses is attached as annex II.

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

    i. 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.

    ii. A specific obligation is added in clause 9(f) with regard to the use of sub-processors and onward transfers. Any onward transfer of personal data will be 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 SCCs as well as, in addition, a provision that these SCCs 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. A copy of the signed contract including these SCCs shall be submitted for information to the data exporter. The same obligation shall also be applicable for any

[1] 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).

onward transfer of personal data to any affiliate or partner of the data importer or a sub-processor.

iii. The exclusive jurisdiction of the CJEU is taken into account with regard to cases brought by a data subject against the institution.

38. While the use of the SCCs as a model for the ad hoc clauses is accepted, the exact wording of the new ad hoc contractual clauses, and especially clause 9(f), are under discussion with Cisco.

5. Signatories to the ad hoc contractual clauses

39. The EDPS wishes that the CJEU concludes the new ad hoc contractual clauses with Cisco International Limited UK and Cisco Systems Inc. US for controller to processor transfers (from the CJEU to Cisco) and processor to processor transfers (between these two Cisco establishments). It should be possible also for other recipients (e.g. other Cisco entities and other sub-processors) 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 CJEU.

40. The new ad hoc contractual clauses for controller to processor transfers are intended to be signed between the CJEU, Cisco Systems Inc., and Cisco International Limited.

41. A docking clause is foreseen in clause 7 for other entities to accede to these clauses, as data exporter (for other EU institutions and agencies) or as data importer (for other Cisco entities or sub-processors). This clause is taken over from the SCCs.

42. As for processor to processor transfers, clause 9 is complemented by points (f) and (g) which contain an obligation that any onward transfer is subject to a contract being signed which includes the SCCs as well as, in addition, a provision that these SCCs prevail over any other contractual obligation. The CJEU also has access to these contracts in order to be able to verify the compliance with this condition.

43. Furthermore, the sub-processor will have to apply technical and organisational measures that, at least, reach the same level of security as those mentioned in a separate exhibit B to the contract, which is applicable also tothe ad hoc contractual clauses. In accordance with clause 9(b), the use of a sub-processor should also be done 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.

44. The CJEU considers that, if accepted, these clauses will offer sufficient guarantees that any onward transfer will respect the level of protection of natural persons guaranteed by the Regulation.

45. The use of the SCCs for the transfer of personal data to a sub-processor in a third country by a processor that is not a Union institution or body is a situation foreseen in consideration 8 of the decision.

46. Furthermore, the use of the SCCs for such onward transfers from processor to processor will eliminate the need for the CJEU and Cisco to adopt specific ad hoc clauses for this situation and for the CJEU to be a party to contractual clauses concluded between Cisco and its different sub-processors.

47. Cisco would also be required to demonstrate that all of its sub-processors are bound by the obligations under the SCCs in case of an onward transfer. Cisco has already stated in this regard

that all the Cisco entities taking part in the processing of personal data for the provision of both WebEx Meetings and TAC services are bound by the terms of those SCCs.

48. This supplementary obligation in clause 9 is still being discussed with Cisco.

6. Binding effect of the ad hoc contractual clauses

49. The EDPS wishes that the CJEU ensures that the provisions of the new ad hoc contractual clauses, including those in the main body of the contract, apply to and are binding upon other Cisco establishments (e.g. Cisco Inc. US), its affiliates, partners and sub-processors and are not rendered ineffective by the concurrent application of other obligations Cisco may impose on them (e.g. intra-corporate agreements).

50. Clause 9(b) on the use of sub processors states that 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.

51. The main contract, furthermore, states that 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 regarding data protection in writing to those parties, including subcontractors.

52. More specifically, in case of an onward transfer, clause 9(f) foresees the specific obligation that the contract with the third party includes a provision that the SCCs used for this transfer prevail over any other contractual obligation.

7. Description of data flows in the contract

53. The EDPS wishes that the new ad hoc clauses clearly detail (e.g. in annexes) in a binding way for Cisco and all sub-processors (whether Cisco entities, its affiliates or other sub-processors) which personal data from which Cisco Webex and related services will be transferred for which purpose to which recipients in which third country with which safeguards and measures.

54. The description of the data flows will be clarified, where necessary, in the light of the answers of Cisco on the remaining question of the CJEU. This description of the transfers of personal data will be included in the annexes to the ad hoc contractual clauses.

8. Measures with regard to other sub-processors and recipients

55. The EDPS wishes that, if the other recipients do not adhere to the new ad hoc contractual clauses concluded by the CJEU, the CJEU obtains sufficient guarantees that Cisco has implemented appropriate contractual, technical and organisational measures with other Cisco establishments (e.g. Cisco Mexico), its affiliates, partners and sub-processors to ensure the required level of protection. The CJEU is to satisfy itself that such measures implemented for transfers to other recipients: i) correspond to the role and the processing of transferred data the recipient will carry out and ii) are in line with the assessments made and supplementary measures identified by the CJEU during the TIA.

56. The measures with regard to the use of other sub-processors or recipients of personal data are described under point 6 above.

9. Disclosure requests

57. The EDPS wishes that the new ad hoc contractual clauses contain clear obligations and binding commitments from Cisco to notify and redirect to the CJEU any disclosure requests for CJEU's data that Cisco, its affiliates or its sub-processors receive from public authorities of a third country, or from another requesting third party in a third country, and to legally challenge such disclosure requests.

58. The obligation for Cisco International Limited, as a party to the main contract, to notify the CJEU of any legally binding request for disclosure of the personal data processed has been maintained.

59. This obligation is complemented in case of transfer of personal data in accordance with the ad hoc contractual clauses, with the obligations foreseen in clauses 14 and 15 of the SCCs, which have been taken over in the ad hoc clauses without modification.

60. These elements, as well as Cisco's Principled Approach, will be taken into consideration while finalising the transfer impact assessment (see point 3).

10. No back door policy

61. The EDPS wishes that the new ad hoc contractual clauses include clauses whereby Cisco certifies that:

    (i) it has not purposefully created back doors or similar programming that could be used to access the system and/or personal data,

    (ii) it has not purposefully created or changed its business processes in a manner that facilitates access to personal data or systems, and

    (iii) that national law or government policy does not require the importer to create or maintain back doors or to facilitate access to personal data or systems or for the importer to be in possession or to hand over the encryption key.

62. The main contract is complemented with the following clause:

    "The Supplier certifies that:

    (i) it has not purposefully created back doors or similar programming that could be used to access the system or personal data;

    (ii) it has not purposefully created or changed its business processes in a manner that facilitates access to personal data or systems, and

    (iii) that national law or government policy does not require the data importer to create or maintain back doors or to facilitate access to personal data or systems or for the data importer to be in possession or to hand over the encryption key."

63. The same clause is also part of the additional commitments that are included in the annexes to the ad hoc contractual clauses.

64. The addition of this clause is still being discussed with Cisco.

11. End-to-end encryption

65. The EDPS wishes that the new ad hoc contractual clauses include clear obligations and commitments that the technical supplementary measures of the use cases 1 and 3 of Annex 2 to

the EDPB Recommendations 01/2020 and fulfilling the conditions for their effectiveness are adopted for all the Webex videoconferencing communications, using state of the art end-to-end encryption technology.

66. Cisco has provided information with regard to the encryption of data in transit and its Zero Trust Security Based End-to-End Encryption for WebEx Meetings. This information is included in annex III.

67. These elements will be part of an annex (Exhibit B) applicable to the main contract as well as to the ad hoc contractual clauses.

12. Pseudonymisation or access to personal data

68. The EDPS wishes that the new ad hoc contractual clauses include clear obligations and commitments that either:

    (i) the technical supplementary measure of the use case 2 of the EDPB recommendations is fully applied in all personal data transferred to Cisco, using state-of-the-art pseudonymisation technologies, or

    (ii) a combination of technical and organisational measures (pseudonymisation, access controls, special training module for administrators etc.) is adopted, so that Cisco effectively does not have access to personal data.

69. Cisco's information security exhibit will be part of the main contract and the ad hoc contractual clauses as a new annex (Exhibit B). The contents of this exhibit is available at https://trustportal.cisco.com/c/r/ctp/trust-portal.html#/1604543381171981.

70. Furthermore, any update of the security measures should be submitted for approval to the CJEU.

13. Access to personal data

71. The EDPS wishes that the new ad hoc contractual clauses include clear obligations and commitments that:

    (i) by default Cisco does not have access to the CJEU data,

    (ii) Cisco will provide remote technical assistance, only in case a Single Point of Contact (SPoC) from the CJEU makes a formal request, and in that case the CJEU will provide manually the minimum amount of anonymized data needed for the resolution of the problem, while Cisco will delete these data upon resolution of the problem;

    (iii) apart from the data received by the CJEU SPoC, Cisco shall not have access to other CJEU data.

72. The main contract is complemented with the following clause:

    "Furthermore, the Supplier certifies that:

    (i) it does not have access by default to the data of the data exporter;

    (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 that it will delete these data upon resolution of the problem, and

(iii) apart from the data received from the data exporter SPoC, it shall not have access to other data of the data exporter."

73. The same clause is also part of the additional commitments that are included in the annexes to the ad hoc contractual clauses.

74. The addition of this clause is still being discussed with Cisco.

14. Training

75. The EDPS wishes that the new ad hoc contractual clauses ensure that specific training procedures for personnel in charge of managing requests for access to personal data from public authorities will be developed, that includes the requirements of EU law as to access by public authorities to personal data, in particular as following from Article 52 (1) of the Charter of Fundamental Rights. Such training should be periodically updated to reflect new legislative and jurisprudential developments in the third country and in the EEA.

76. The main contract is complemented with the following clause:

"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."

77. The same clause is also part of the additional commitments that are included in the annexes to the ad hoc contractual clauses.

78. The addition of this clause is still being discussed with Cisco.

ANNEXES

I. Draft ad hoc contractual clauses

II. Cisco information with regard to encryption

Mr Wojciech Rafał Wiewiórowski
European Data Protection Supervisor
Rue Wiertz 60
1047 Brussels
BELGIUM

edps@edps.europa.eu

Luxembourg, 25 February 2022

BY E-MAIL

Your reference: C 2021-0255

Intermediate compliance report on the implementation of the conditions set for the renewal of the authorisation for the use of ad hoc contractual clauses for the transfer of personal data

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 is to provide to the EDPS an intermediate compliance report demonstrating steps taken to implement the conditions set for the renewal of the authorisation. Please find enclosed said report.

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:

- Intermediate compliance report on the implementation of the conditions set for the renewal of the authorisation for the use of ad hoc contractual clauses for the transfer of personal data
- Annex I to the report – Draft ad hoc contractual clauses
- Annex II to the report – Cisco information with regard to encryption

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

3) Cisco International Limited
Cisco International Limited agrees that this Exhibit A and its Annexes are an integral part of the Agreement and its Amendment. Any obligation on the Processor towards the Controller resulting from this Exhibit A and its Annexes is part of the contractual obligations of the Supplier towards the Customer.
Signature and date:

_____

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 B 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 B. 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 B.

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 Annex 2 to this Exhibit A. 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 six (6) months in advance, 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 Standard Contractual Clauses adopted by Commission Implementing Decision (EU) 2021/914 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. A copy of the signed contract including these Standard Contractual Clauses is submitted for information to the data exporter. The sub-processor shall apply technical and organisational measures that, at least, reach the same level of security as those mentioned in Exhibit B.

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 B 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

This Annex 1a "Cisco WebEx Meetings" forms an integral part of the *Ad Hoc* Contractual Clauses in Exhibit A.

The data importer submits any update in the processing operations detailed in this Annex 1a for approval to the data exporter. 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

Under discussion with Cisco

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 that:

   i. it has not purposefully created back doors or similar programming that could be used to access the system or personal data,

   ii. it has not purposefully created or changed its business processes in a manner that facilitates access to personal data or systems, and

   iii. that national law or government policy does not require the data importer to create or maintain back doors or to facilitate access to personal data or systems or for the data importer to be in possession or to hand over the encryption key.

2. The data importer certifies that it does not have access by default to the data of the data exporter.

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

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

The data importer submits any update in the processing operations detailed in this Annex 1b for approval to the data exporter. 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

Under discussion with Cisco

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 that:

   i. it has not purposefully created back doors or similar programming that could be used to access the system or personal data,

   ii. it has not purposefully created or changed its business processes in a manner that facilitates access to personal data or systems, and

   iii. that national law or government policy does not require the data importer to create or maintain back doors or to facilitate access to personal data or systems or for the data importer to be in possession or to hand over the encryption key.

2. The data importer certifies that:

   i. it does not have access by default to the data of the data exporter,

   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 that it will delete these data upon resolution of the problem, and

   iii. apart from the data received from the data exporter SPoC, it shall not have access to other data of the data exporter.

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 2 To Exhibit A

List of Sub-processors

Under discussion with Cisco

Exhibit B

Information Security Exhibit

Under discussion with Cisco

Cisco information with regard to encryption

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.

- 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 signaling.

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 signaling 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
- PSTN Call-in/Call-back