EUROPEAN DATA PROTECTION SUPERVISOR

# EDPS Decision temporarily and conditionally authorising the use of contractual clauses between the Court of Justice of the EU and Cisco Systems Inc. US for transfers of personal data in the Court's use of Cisco Webex and related services

## 28 October 2022

## (Case 2022-0902)

*Summary:*

This Decision addresses the request from the Court of Justice of the EU (the 'Court') for the renewal of the authorisation of the contractual clauses pursuant to Article 48(3)(a) of (EU) 2018/1725 (the 'Regulation')[1]. Pursuant to Article 57(1)(e) and Article 58(3)(e) of the Regulation, the EDPS authorises until 31 October 2024 the use of contractual clauses between the Court of Justice of the EU and Cisco Systems Inc. US as a means for adducing appropriate safeguards under Article 48(3)(a) of the Regulation in the context of transfers of personal data in the Court's use of Cisco Webex and related services, given the Court's progress in its compliance with the Conditions of the EDPS Authorisation Decision of 31 August 2021.

The Court is to ensure an essentially equivalent level of protection within 16 months as of the date of this Decision, i.e. 1 March 2024, by remedying the compliance issues identified in the present authorisation.

The Court is to provide the EDPS an intermediate compliance report 12 months after the date of this Decision, i.e. 1 November 2023, demonstrating steps taken to implement the conditions set in this Decision, as well as a final compliance report at the expiry of the 16-month deadline to comply.

[1] 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, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC, OJ L 295, 21.11.2018, p. 39.

EUROPEAN DATA PROTECTION SUPERVISOR
Postal address: rue Wiertz 60 - B-1047 Brussels
Offices: rue Montoyer 30 - B-1000 Brussels
E-mail: edps@edps.europa.eu
Website: edps.europa.eu
Tel.: 32 2-283 19 00 - Fax: 32 2-283 19 50

Table of Contents

# 1. PROCEEDINGS

1.1. This Decision concerns the renewal of the EDPS Authorisation Decision of 31 August 2021[2] of contractual clauses concluded between the Court of Justice of the EU ('the Court') and Cisco Systems Inc. US in the context of transfers of personal data in the Court's use of Cisco Webex and related services.

1.2. In order for the Court to provide appropriate safeguards ensuring an essentially equivalent level of protection with regard to international transfers of personal data to Cisco or its sub-processors, including by remote access, the EDPS set **14 Conditions** that the Court was required to meet **for the renewal of the authorisation**.[3]

1.3. The Court was required to ensure the compliance with the Conditions set in the EDPS Authorisation Decision of 31 August 2021 within one year from the date of that Decision.

1.4. On 1 September 2022, the Court submitted a letter requesting the renewal of the EDPS authorisation in accordance with Article 48(3)(a) of the Regulation. The Court attached two Annexes to the letter. Annex I consists of the draft Supplementary Agreement No. 1 to 'CISCO and Court of Justice of the European Union Enterprise License Agreement (ELA)', accompanied by four exhibits:

1. Exhibit A: ' Contractual Clauses' (' 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' with its
    a. Attachment 1: 'Webex Meeting Privacy Data Sheet',
    b. Attachment 2: 'TAC Privacy Data Sheet'.

Annex II consists of 'Data Transfer Impact Assessment for the Use of CISCO Webex by the Court of Justice of the European Union' ('TIA').

1.5. On 30 September 2022, the EDPS issued a Decision which prolonged the effects of the EDPS Authorisation Decision of 31 August 2021 until 31 October 2022.

1.6. The EDPS issues this Decision in accordance with Article 57(1)(n) and Article 58(3)(e) of the Regulation.

1.7. This Decision is addressed to the Court of Justice of the EU.

---

[2] EDPS Decision authorising temporarily the use of contractual clauses between the Court of Justice of the EU and Cisco for transfers of personal data in the Court's use of Cisco Webex and related services, 31 August 2021 (Case 2021-0255), available at https://edps.europa.eu/system/files/2021-11/17-11-2021-edps_decision_authorising_temorarily_use_of_cjeu-cisco_ad_hoc_clauses_for_transfers_cisco_webex_1.pdf.

[3] The conditions are listed under Section 3 of this Decision.

# 2. BACKGROUND INFORMATION - ANALYSIS OF THE FACTS AS UNDERSTOOD BY THE EDPS

2.1. The Court concluded a contract (the Enterprise License Agreement - 'ELA') with Cisco International Limited UK ('the contract'), with certain annexes concluded with Cisco Systems Inc. US. The contract provides for the use of Cisco software on premises (Cisco Video Mesh, Cisco Meeting Server, Cisco Unified Communications Manager), as well as the provision of Cisco cloud services (Cisco Webex Meetings, Cisco Webex Events) and maintenance/support services (Cisco Technical Assistance ('TAC') Service Delivery).[4]

2.2. The current draft of the Supplementary Agreement is to be signed between the Court and Cisco International Limited UK (named as a Supplier), while the contractual clauses, constituting Exhibit A to that Agreement, between the Court and Cisco Systems Inc. US (named as a processor).

2.3. Under Article 2 of the Supplementary Agreement, this Agreement forms an integral part of ELA and shall enter into force on the date when the last party to ELA signs it. Where there is a conflict between the terms of the ELA and the Supplementary Agreement, the terms of the Supplementary Agreement shall prevail with respect to its subject matter. Where the provisions of the original ELA are not modified by the terms of the Supplementary Agreement, they remain unchanged and shall continue to apply.

2.4. Under Article 1(1) of the Supplementary Agreement, its purpose is to address the requirements set out in the EDPS Authorisation Decision of 31 August 2021.

2.5. To this end, Article 1(4) of the Supplementary Agreement removes the previous version of Article 11(2) of ELA and replaces it in full with a new wording. It specifies, inter alia, Cisco International Limited UK obligations as regards the processing of personal data in general, as well as those concerning international transfers. In particular, Article 1(4) inserts new obligations of Cisco International Limited UK concerning requests for disclosure, access rights, binding obligations vis-a-vis Cisco's sub-processors, and training procedures for certain personnel.

2.6. When it comes to the contractual obligations of Cisco International Limited UK, which is the signatory of the Supplementary Agreement, and Cisco Systems Inc. US, which is the signatory of the contractual clauses, Article 1(4)(d) of the Supplementary Agreement specifies that Cisco International Limited UK is bound by the same obligations as Cisco Systems Inc. US under the contractual clauses. Hence, the obligations on the Cisco Systems Inc. US, acting as a processor receiving

[4] This information was provided to the EDPS in the context of the EDPS Authorisation Decision of 31 August 2021.

transfers, are also part of contractual obligations of Cisco International Limited UK under ELA.[5]

2.7. Based on the TIA, the following is meant under the specific categories of data referenced throughout the documents provided by the Court:

- **User Information** refers to Name, E-mail Address, Password, Browser, Phone Number, Mailing Address, Avatar, User Information Included in Your Directory, and the Unique User ID ('UUID');
- **Host and Usage Information** refers to 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** refers to Meeting Recordings, Transcriptions of meeting recordings, Uploaded Files. In this context, in Cisco's understanding, this category **does not seem to include the real-time meeting data** such as VoIP, video and high frame rate sharing data;[6]
- **TAC support Information** refers to 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 Attachments data** refers to files provided by customers that might contain personal data.

2.8. The videoconference services provided by Cisco Webex entail the processing of personal data under three separate sub-services:

- Signalling that uses User Information as well as Host and Usage Information,
- Transmission of real-time meeting data, and
- Processing of static User-Generated Information.

2.9. Based on the clarifications of the Court, the **Billing data** is understood as the host name and e-mail address, the meeting site URL, the Meeting start and end time as well as the telephone number. Billing data is hence part of the categories User information and Host and Usage information. The **Analytics data** is understood as

[5] Article 1(4)(d) of the Supplementary Agreement reads: '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.'

[6] However, it appears that 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.

User Information and Host and Usage Information used to provide analytics and statistical analysis in aggregate form and to improve the technical performance of the Service.[7]

2.10. According to the statements provided by the Court in the TIA,[8] the following functionalities and elements of the **Webex Suite** are relevant for the use by the Court:

- Webex Meetings (videoconference technology),
- Webex Webinars (seminars and conferences through a videoconference with a larger number of participants),
- Webex Events (organisation of in-person, hybrid, and virtual events).
- Webex Calling (calls by using the Cloud infrastructure).
- Webex Messaging (send messages by using the Cloud infrastructure).
- Slido (polling, quizzes or other feedback during a videoconference).

2.11. Also according to the TIA, the use of Webex Events, Webex Calling, Webex Messaging and Slido are disabled at the Court.[9]

2.12. According to the TIA, the **Webex App**, installed on the Court's users' computers, provides the integration of Webex Calling, Meetings and Messaging in a single application. The Webex App, understood to be installed in Court's devices, also allows for the use of WebEx Zero Trust Security End-to-End encryption[10] and Private Meetings[11]. According to the TIA, the Webex App installed in Court's devices will be the only authorised by the Court to access Webex Meetings. According to the Court, when the Webex App is used to access meetings, given the technical configuration and adjustments Cisco has made, personal data will stay in the EU.[12]

2.13. Based on the TIA, international transfers of personal data may take place to the United States, United Kingdom, Brazil, Australia, Japan, Singapore, India or Jordan. The transfers take place on the basis of the relevant adequacy decisions in the case of the United Kingdom and Japan. The remaining transfers taking place to the other countries are based on the use of contractual clauses.

2.14. As part of the original commitments, Cisco committed itself to implement the so-called '**Webex Data Residency for EU countries'**. This programme was to ensure that the personal data processed as part of Cisco Webex services are stored and processed in the EU/EEA. In the TIA, the Court informed the EDPS that this programme has been deployed and that since August 2021, **the main data centre**

[7] Para 36 of the TIA.
[8] Which is, however, not reflected in the Supplementary Agreement.
[9] Para 10 of the TIA.
[10] See Section 3.1.11 of this Decision.
[11] See point 2.46 of this Decision.
[12] Para 11 of the TIA.

**where the data from the Court is '*processed*' is located in Frankfurt, Germany, with a back-up data centre in Amsterdam, The Netherlands**.[13]

2.15. According to Annex 1a to Exhibit A, the Webex Data Residency programme '*provides Customer* [the Court's] *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* [...] (emphasis added).'[14]

2.16. In this context, **the remit and consequences of the deployment of the Webex Data Residency programme for the Court's use of Cisco Webex and related services remain unclear.** The Cisco Webex' public explanation on the Data Residency in the Webex App makes a distinction between '*storage'* and '*processing'* of data, and indicates the level of security of the residency program per type of processing operations and category and type of personal data processed. Notably, Cisco Webex identified three levels of data residency: a) Global where data may be handled at a Cisco data centre in any location, b) Limited where data resides in the organization's geographic region, but copies may be created or processed in other regions as needed, and c) Restricted where data resides in the organization's geographic region.[15] The Court did not provide similar specific information to the EDPS regarding the scope of the Webex Data residency programme. It did not provide crucial information, such as identification if the programme covers 'storage' and 'processing' following Cisco's distinction of processing activities, as well as the notion of User-Generated Information. In addition, it is not clear what types of personal data are covered under the programme.[16] It is also not clear how this programme is deployed in the Court's use of Webex Cisco and related services.

**Processing for the Court's use of Cisco Webex services**

2.17. The Court informed the EDPS that the Webex Data Residency programme covers the billing data, analytics data[17] and data processed in the context of Hybrid Calendar Service. However, it is unclear whether the transfers of the billing data have stopped. In its TIA, the Court asserted that no transfer of personal data takes place for billing purposes after July 2022.[18] However, Exhibit D, Attachment 1, Section 4, states that '*until August 2022, some Host and Usage information will continue to incur cross-border transfers outside of the region, for billing purposes'*. The

[13] Para 23 of the TIA.
[14] Page 24 of Annex 1a of Exhibit A.
[15] Webex' explanation on the Data Residency in Webex App available at https://help.webex.com/en-us/article/oybc4fb/Data-residency-in-Webex-App, [accessed 30 September 2022].
[16] For instance, it is unclear if the so-called 'operational data', as described by the Court in the context of the EDPS Authorization Decision of 31 August 2021 (point 2.10), is covered by the Webex Data Residency programme.
[17] Both billing and analytics data overlap with the Host and Usage Data, and User Data. See point 2.9 of this Decision.
[18] Para 31 of the TIA.

Court does not explain this discrepancy resulting from the overlap between the billing data with Host and Usage Information.[19] Hence, it is unclear what specific data is covered under the billing data for which the Court claims that transfers had stopped.[20]

2.18. For **the analytics data**, the Court asserted that due to the deployment of the Webex Data Residency, transfers of personal data for analytics purposes were eliminated after July 2022, and that, according to the Court, includes transfers following remote access to analytics data.[21]

2.19. For **Hybrid Calendar Service**, the Court asserted that '[t]*he 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*'.[22]

2.20. However, according the Supplementary Agreement (Annex 1a to Exhibit A), **there are exceptions to the deployment of the Webex Data Residency programme**, most of which are not related to the use of Web Meetings as such. As a result, there are still transfers of personal data taking place in the context of Cisco Webex services.[23] The **Court asserts that the processing of personal data '*largely*' takes place within the EU/EEA**, but some transfers might occur '*through specific actions or use of functions by the user administrator or user*' or '*as a result of the use of third-party sub-processors*'.[24]

2.21. The transfers that still take place are either directly to Cisco Systems Inc. US, or onward transfers from Cisco International Limited UK's servers in Frankfurt or Amsterdam to Cisco Systems Inc. US or its sub-processors.[25] If the transfers take place, they involve the following categories of personal data: User Information, Host and Usage Information, and User Generated Information.[26]

2.22. With regard to **the transfers still taking place because of '*specific actions or use of functions by the user administrator or user*'**, the transfers may occur when:

(i) *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*;

[19] Point 2.9 of this Decision.
[20] Para 34 of the TIA.
[21] Para 35 of the TIA.
[22] Para 41 of the TIA.
[23] Para 42-59 of the TIA, and pages 24-26 of Annex 1a to Exhibit A.
[24] Paras 27-29 of the TIA.
[25] Interpretation of the flowchart included in para 30 of the TIA.
[26] For more detailed identification of the personal data involved, see pages 24-26 of Annex 1a to Exhibit A. However, the EDPS underlines that at present the notion of User-Generated Information in the Court's understanding remains unclear (see point 2.7 of this Decision).

(ii) *Customer provides ordering information (business contact information)*;

(iii) *a user engages in collaboration with users outside of the EU region*;

(iv) *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)*;

(v) *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)*.[27]

2.23. The Court asserted that it had taken **organisational measures to avoid or limit the above transfers** taking place because of specific actions or functions.[28] The below sections refer to situations in point 2.22 letter (i)-(iii) and (v), while the situation described in letter (iv) is analysed in point 2.35.

2.24. With respect to the possible transfers due to the situations listed in point 2.22 (i), the Court explained that the users of the Court do not need to register themselves on any Cisco platform or a Cisco service in order to use Webex. The Court further explained that external users are also not required to perform such a registration.[29]

2.25. With respect to the possible transfers due to the situations listed in point 2.22 (ii), the Court explained that the ordering information for the use of Webex by the users of the Court is handled in the contract. No further business contact information is required for the use of Webex by the Court.[30]

2.26. With respect to the possible transfers due to the situations listed in point 2.22 (iii), the Court explained that '*specific collaborations tools'* such as Webex Calling or Webex Messaging are not used by the Court. Furthermore, the Court stated that it will use only media nodes located in the EU.[31]

2.27. With respect to the possible transfers due to the situations listed in 2.22 (v), the Court explained that the Court blocks optional functionalities that might necessitate a transfer of personal data without appropriate safeguards when the Court is aware of the functionality and that functionality can be blocked. The Court explained that such functionalities are third party telephony, third party applications via Webex App hub or third-party application stores (Slido).[32]

---

[27] Para 41 of the TIA, page 24 of Annex 1a to Exhibit A and Point 4 of Attachment 1 to Exhibit D.
[28] Para 43 of the TIA, and paras 127-128 of the TIA.
[29] Para 127(a) of the TIA.
[30] Para 127(b) of the TIA.
[31] Para 127(c) of the TIA.
[32] Para 127(e) of the TIA.

In addition, the Court explained that 'push' notifications can be configured locally on mobile devices of users, and hence cannot be entirely controlled by the Court. The Court stated that it does, however, impose that, in principle, only professional devices are used for work related communications.[33]

2.28. With regard to **the transfers still taking place because of *the use of third party sub-processors,*** the Court stated that '[w]*hile 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.*'[34]

2.29. In the TIA as well as Exhibit B, the Court includes references to sub-processors whose use could result in transfers, but which sub-processors are, according to the Court, not used by Cisco in the Court's use of Webex services. This concerns services provided by **Walkme, Inc**.[35] - software that the Court claims that it disabled which provides a step-by-step guidance on how to use Webex online. It also concerns services provided by **Vbrick**, whose services are, according to the Court, used only when videoconferencing capacity exceeds more than 3 000 participants, while the Court's licence allows for a maximum of 1 000.[36] In case of these sub-processors, **no transfers effectively take place** since Cisco Webex does not use the services of the mentioned sub-processors when delivering the services to the Court.

2.30. In the TIA as well as Exhibit B, the Court stated that Cisco Webex uses **AWS** 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.[37] That processing done by AWS can take place in the United States, the United Kingdom, Brazil, Australia, Japan, Singapore or the EU. According to the Court, under Cisco's Webex Data Residency programme, AWS '*has taken measures*' to process in the EU the data of Webex Meeting customers which were provisioned in the EU, and asserted that Cisco's encryption methods preclude AWS from having access to this raw data in the clear.'[38] However, the information provided by the Court does not specify how and to what extent AWS could and did implement Cisco's Webex Data Residency program[39], and what encryption methods are employed by Cisco to preclude access from AWS.

2.31. According to the Court, the AWS cloud infrastructure is also used to host **Webex media nodes** that may process real-time meeting data such as VoIP, video and high

[33] Para 127(f) of the TIA.
[34] Para 44 of the TIA. The EDPS notes that these exceptions were not disclosed in Annex 1a to Exhibit A.
[35] Para 47 of the TIA.
[36] Para 50 of the TIA.
[37] Para 53 of the TIA.
[38] Paras 55-56 of the TIA.
[39] On its website, AWS states that 'You can also use AWS services with the confidence that customer data stays in the AWS Region you select. A small number of AWS services involve the transfer of data, for example, to develop and improve those services, where you can opt-out of the transfer, or because transfer is an essential part of the service (such as a content delivery service).' Available at https://aws.amazon.com/compliance/eu-data-protection/ [accessed 20 September 2022].

frame rate sharing data.[40] According to the Court, the users are able to connect to the closest media node for better performance, and the processing by AWS can be located in the United States, the United Kingdom, Brazil, Australia, Japan, Singapore or the EU. The Court asserted that **it imposes the use of media nodes located within the EU/EEA through the deactivation of Global Distributed Meetings**.[41] In addition, the Court asserted that '[t]*he use of media nodes located solely within the EU/EEA* ***avoids a transfer*** *of personal data to media nodes located outside the EU/EEA*' (emphasis added).[42] As informally specified by the Court in its reply to a request for clarification from the EDPS, this implies that Webex Meetings users located out of the EU/EEA and participating in a videoconference organised by the Court will also connect to a media node located in the EU/EEA. At the same time, the Court added that '[t]*he 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*' (emphasis added).[43] The Court does not specify whether and to what extent transfers take place when the media nodes provided by AWS are used by Cisco Webex.

2.32. As explained by the Court in the TIA, the use of Akamai Technologies Inc. as a sub-processor **continues to result in transfers to third countries**. The Court stated that Cisco Webex uses **Akamai Technologies, Inc.** as a content delivery network for static content. Based on the provided information, the data sent to Akamai Technologies, Inc. would '*initially*' be located in the EU, i.e., in the data centre in Frankfurt, Germany, with back-up in Amsterdam, the Netherlands.[44] However, in order to create logs, which can be used for instance for troubleshooting, the Court indicated that Akamai Technologies, Inc. may process the IP address, browser and geographic region of a user. Those logs may be transferred to the United States.[45]

**Processing for the Court's use of Cisco Technical Assistance ('TAC') Service Delivery**

2.33. As mentioned above in point 2.22, **the transfers of personal data still take place because of '*specific actions or use of functions by the user administrator or user*'**, inter alia when 'technical support is requested through Cisco's TAC, in which case the information that a user provides within the initial TAC request may be transferred outside the EU/EEA.[46] According to the Court, the use of TAC support leads to the processing of TAC Support Information and the Customer case attachments, which may include personal data. In any case, to provide support, Cisco can access and process User Information as well as Host and Usage Information.[47] The Court informed that the personal data included in the Customer

[40] Para 102 of the TIA.
[41] Para 100 of the TIA.
[42] Para 103 of the TIA.
[43] Para 59 of the TIA.
[44] Para 51 of the TIA.
[45] Para 52 of the TIA.
[46] Para 41(d) of the TIA, and page 24 of Annex 1a to Exhibit A.
[47] Para 60 of the TIA.

case attachments is under its control as it decides what data should be included.[48] In addition, because of the use of the Hybrid Calendar Services, this information may also include user identifiers (UUID). However, the information with regard to meetings without Webex is end-to-end encrypted when transmitted 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.[49]

2.34. According to the TIA, the TAC support information and Customer case attachments are transferred in all situations to the United States: to Salesforce for TAC support information, and to AWS for Customer case attachments.

2.35. The Court asserts that it has taken **organisational measures** to limit or avoid transfers of personal data outside of the EU/EEA in the context of TAC requests by ensuring that its users do not directly open a support case.[50] When support is needed, the Court's users must first contact the internal helpdesk of the Court, which will then, if required, contact Cisco. According to the Court, 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)*'. Furthermore, as the Court asserted that it will open support cases during EU business hours, these support cases will '*initially*' be dealt with by Cisco entities within the EU (through EU media nodes under the so-called 'follow the sun' practice).[51]

2.36. With regard to **technical supplementary** measures previewed by the Court, the Court explained that TAC Support Information and Customer case attachments are only accessed by Cisco, and that no personnel from third-party service providers have access to this data.[52] What is more, in the TIA the Court stated that '[c]*ustomer case attachments are, furthermore, considered customer data and are encrypted both in transit and at rest by Cisco*'.[53] Additionally, according to the Court, '*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*'.[54] In a reply to a request for clarification, the Court stated that '[i]*t is the understanding of the CJEU that TAC support information is* ***not encrypted at rest****. Other security measures are, however, in place, such as authentication, access controls activity logging and monitoring as well as data masking*' (emphasis added).

2.37. In that request, the EDPS asked also about how and by whom the keys used to encrypt the TAC Support Information in transit and the Customer case

[48] Para 61 of the TIA.
[49] Para 62 of the TIA.
[50] Para 127(d) of the TIA.
[51] Paras 139-141 of the TIA.
[52] Para 63 of the TIA.
[53] Para 64 of the TIA.
[54] Para 89 of the TIA.

attachment(s) at rest are generated and managed. In the reply the CJEU stated that '[t]he *keys for encryption are managed by Cisco, but the communication is done via CJEU VPN which adds another layer of encryption*'.[55]

2.38. The Court further explained that 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 linked with the so-called 'follow the sun approach' where 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. In such a case, a transfer can take place to the United States, the United Kingdom, India or Jordan.[56]

2.39. Based on the flowchart provided in the TIA, **in the context of TAC requests, transfers occur either directly between the Court and Cisco's support locations (affiliates) and third party sub-processors** (Salesforce and AWS), but **also indirectly from the processor's data centres in Frankfurt and Amsterdam to Cisco's support locations (affiliates) and third party sub-processors** (Salesforce and AWS).[57]

2.40. As an organisational measure, the Court indicated that TAC support customers should call Cisco TAC support during the standard EU business hours because this way case their case is more likely handled by TAC support within the EU. The Court also indicated that its users can minimise personal data transfers by minimising the personal data reflected in the case attachments.[58] The EDPS provides his analysis of the effectiveness of these measures in Sections 3.1.11 - **Condition 12** and 3.1.12 - **Condition 13**.

**Other supplementary measures implemented by the Court**

2.41. In the TIA, the Court identified supplementary measures that it considers appropriate and necessary for transfers in the Court's use of Cisco Webex Meeting and related services. In this respect, some of the supplementary measures, especially the organisational ones, identified by the Court in the TIA are not reflected in the Supplementary Agreement, nor its exhibits.[59]

2.42. The **technical measures** encompass encryption of data in transit, Webex Zero Trust Security End-to-End Encryption, and usage of media nodes located in the EU. The EDPS analyses these measures and their effectiveness under Section 3.1.10 - **Condition 11**.

[55] Point 5 of the Court's answer of 15 September 2022.
[56] Para 65 of the TIA.
[57] Para 67 of the TIA.
[58] Para 66 of the TIA.
[59] In particular with regard to the Court's technical choices, see Sections 3.1.10 - Condition 11, and 3.1.11 - Condition 12.

2.43. The **contractual measures** encompass a docking clause (analysed under Section 3.1.5 - **Condition 5**), transparency obligations and obligations to take specific actions (analysed under Section 3.1.8 - **Condition 9**), prohibition of back door policies (analysed under Section 3.1.9 - **Condition 10**), access controls to the data (analysed under Section 3.1.12 - **Condition 13**), specific training procedures (analysed under Section 3.1.13 - **Condition 14**) and obligation to pass on essentially equivalent safeguards to further processors (analysed under Sections 3.1.6 and 3.1.7 - **Conditions 6, 7 and 8**).

2.44. The **organisational measures** encompass limitations on the actions from users or user administrators to avoid transfers of personal data outside of the EU/EEA (explained under points 2.23-2.28 and 2.40), use of alternative solutions such as Cisco Meeting Server and streaming service (explained under point 2.45), use of Private Meeting function (explained under point 2.46), as well as measures enabled by Court to limit personal data transmission (explained under point 2.47), limitations on the opening of a support case (explained under point 2.40) and other Court's internal policies (explained below under point 2.48).

2.45. With regard to the possible use of **alternative solutions** to Cisco Webex, the Court indicated that it does not only use Webex for videoconferencing, and that for meetings or conferences requiring a higher level of security, the Court plans to use the Court's **Cisco Meeting Server**, where '*all data is processed on premises*'.[60] Assuming that the User Generated Data includes the real-time meeting data, and is processed under the control of the Court, and that the Court applies appropriate information security measures on their IT infrastructure in line with current security best practices (physical, network, access control, etc.), the access by Cisco in the Court's use of Cisco Meeting Server can be regarded as not technically feasible. Further, the Court indicated that for events that require the ability for a large number of people to follow the event remotely, without active participation, the Court can use a streaming service provided by **another provider**.[61] As the Court explained, 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 Court.[62]

2.46. Another organisational measure introduced by the Court is its reliance on **Private meeting** or **Cisco Video Mesh**. According to the Court, videoconferences among the Court's users (either in the office or teleworking with the material provided by the Court) will be '*processed on premises'* with the use of Private Meeting and Cisco Video Mesh. Nevertheless, the **processing on premise does not prevent the transfers**, since, as the Court explained, the User Information and Host and Usage information '*is sent to the cloud and can, therefore, be the object of a transfer of personal data*'.[63] It is **unclear how this is done in practice**.

[60] Para 130 of the TIA.
[61] Para 131 of the TIA. The Court provided no additional information concerning these alternative providers.
[62] Para 132 of the TIA.
[63] Para 134-135 of the TIA.

2.47. Another organisational measures introduced by the Court is its implementation of the following policies.

With regard to User Information:

- for the phone number, mailing address, password and user information included in the Court's directory, the Court uses an identity provider (F5) to identify the users of the Court and transmit their data to Cisco through a SAML protocol. Hence, according to the Court, the personal data transmitted is restricted to the name and e-mail address,
- for the avatar, the Court allows its users to choose it themselves, and if no choice is made, the avatar is not processed.

With regard to the Host and Usage Information:

- for internal users' IP Addresses and IP Addresses along the Network Path, including internal users connected remotely, the Court will use the IP addresses of the Court,
- for call attendee information, including email addresses, username, phone numbers and room device information, the Court will: a) not require a user name for external users in a manner allowing for the identification of a physical person unless this is required for the proper conduct of the meeting or event organised; b) not require external users to provide the email addresses, phone numbers or room device information when joining a meeting. In addition, according to the Court, meetings are conducted with VOIP only, which avoids transmission of phone numbers to conduct a Webex meeting.[64]

2.48. The last organisational measure introduced by the Court encompass Court's **internal policies and guidelines** issued to its staff. These will include instructions and rules on the choice of tools for videoconferencing, on the potential use of private devices for videoconferencing; 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. The Court will also update documentation and information notice which will be provided internally and externally, including the technical requirements for the use of Webex Zero Trust End-to-End Encryption.[65] There is **no indication as to when** these policies will be implemented in practice.

[64] Para 138 of the TIA.
[65] Para 142 of the TIA.

# 3. LEGAL ANALYSIS

## 3.1. Assessment of the implementation of the Conditions

### 3.1.1. Condition 1: Mapping data flows

3.1. In the EDPS Authorisation Decision of 31 August 2021, the EDPS took the view that the contract did not provide clear information on what personal data is likely to be transferred to which recipients in which third countries covered in the contract. The EDPS therefore took the view that the initial safeguards and measures in the contract do not appear to be based on all the information necessary for the Court to fully assess all the risks concerning international transfers and implement appropriate safeguards.[66] The EDPS hence required that the Court 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.[67]

3.2. The Court has identified what personal data is likely to be transferred to which recipients in which third countries covered in the contract in both the TIA and the contractual clauses. The TIA submitted by the Court assessed the data flows between the Court and Cisco International Ltd. UK and Cisco System Inc. US, and its sub-processors.[68] While the Court mapped the data flows in the TIA, the **EDPS has doubts** whether, considering the unclear scope of the Webex Data Residency programme[69], the Court comprehensively captured all of the data flows involved in its use of Cisco Webex and related services.

3.3. Basing on the information provided by the Court, EDPS considers that the Court has **substantially complied with Condition 1.**

### 3.1.2. Condition 2: No transfers of or remote access to personal data

3.4. In the EDPS Authorisation Decision of 31 August 2021 the EDPS requested that all personal data in the Court's use of Cisco Webex services, i.e. user information, host and usage information, user generated information, billing data and analytics data, is stored/resided in the EU, in accordance with the contract concluded between the Court and Cisco. In particular, Webex meeting and connection data (including personal data) in the Court's use of Cisco Webex services (whether on-premises or cloud-based) is stored/resides in the EU and for cloud-based Cisco Webex services no transfers of that data, including by remote access, occur due to Cisco's reliance on data centre services provided by AWS.[70]

[66] Point 3.10 of the EDPS Authorisation Decision of 31 August 2021.
[67] Condition 1 of the EDPS Authorisation Decision of 31 August 2021.
[68] Also in Exhibit A, with its Annexes 1a and 1b, as well as Exhibit B.
[69] See point 2.16 and Section 3.1.2- Condition 2 of this Decision.
[70] Condition 2 of the EDPS Authorisation Decision of 31 August 2021.

3.5. In the first place, based on the above understanding of the facts presented by the Court and explained points 2.14 - 2.19, the EDPS notes that the Court **appears to have migrated the Court's data to the data centres located in the EU**. Based on the information from the Court, this migration covered in particular personal data processed by Webex Meetings, including User Information, Host & Usage Information, and User-Generated Information.[71] Notably, the Court in its TIA clarified that the Webex Data Residency programme covers the billing data, analytics data and data generated in the use of Hybrid Calendar Service.[72]

3.6. In the second place, the EDPS notes that even when data is covered under the Webex Data Residency programme, **the remit and consequences of the Webex Data Residency programme remain unclear**.[73] Notably, as mentioned, the specific types of personal data covered under this programme is unclear. In addition, it is unclear what type of processing operations are included and whether the migration of the data to the EU data centres excludes remote access by sub-processors. Hence, even when, according to the Court, specific data is '*stored*' in the data centres located in the EU, the **EDPS is unable to definitively ascertain whether, in addition to storage, other processing operations are concerned, and what specific types and categories of personal data are covered, and with what consequences**. Under the principle of accountability, the **Court must be able to demonstrate** and substantiate the assertions it makes with regard to putting an end to specific transfers in the context of its use of Webex Cisco and related services. In addition, the EDPS recommends that the Court **perform a detailed reassessment of the mapping of the data flows**.

3.7. What is more, both the TIA[74] and Annex 1a to Exhibit A of the Supplementary Agreement[75] indicate that **there are exceptions to the application on the Webex Data Residency programme** (for some of which the Court identified organisational supplementary measures[76]). The personal data transferred in that context includes User Information, Host and Usage Information as well as User Generated Information.[77] In this context, as noted above in point 2.22 above, where exceptions apply, transfers of personal data take place.

3.8. In addition, the EDPS notes that it **remains unclear whether transfers take place due to Cisco's reliance on data centre services provided by AWS**, with regard to the signalling services,[78] and reliance on AWS' media nodes.[79]

---

[71] Page 24 of Annex 1a of Exhibit A.
[72] See points 7-2.19 of this Decision.
[73] See points 2.16 of this Decision.
[74] Paras 27-29 of the TIA. See also point 2.20 of this Decision.
[75] Page 24 of Exhibit A.
[76] See Section 2 of this Decision.
[77] Pages 25-26 of Exhibit A.
[78] See points 2.30 of this Decision.
[79] See point 2.31 of this Decision. The information provided by the Court seems contradictory because the Court indicated, on the one hand, that no transfers take place, but on the other that the transfers are encrypted.

3.9. Even if the personal data was stored and processed in the data centres located in the EU, the **EDPS highlights that such data localisation in the EU *in itself* and *on its own* does not preclude risks of remote access**, in particular in the context of **third countries' public authorities possible access to data stored (and processed) in the EU**. The EDPS takes the view that the Court should have assessed, and if found to be present, properly mitigated, the risk of unauthorised disclosure as a result of third-country laws with extra-territorial reach.

3.10. This is particularly relevant because the **Protocol No. 7 to the Treaties on the Privileges and Immunities of European Union**, establishes in its Article 2 the inviolability of the archives of the Union. The principle of the inviolability of the archives of the Union applies to the archives of the EU institutions, offices, bodies or agencies, including data stored and processed on their behalf. This entails that cloud service providers, such as AWS, cannot disclose personal data entrusted to them by EU institutions to law enforcement authorities[80], unless the EU institution concerned agrees to disclosure or the disclosure is authorised by the EU judicature as clarified by the case-law of the Court[81]. The objective of the Protocol is functional, inasmuch as it is intended to avoid any interference with the functioning and independence of the European Union. In that regard, the principle of the inviolability of the archives is relied upon by an EU institution in order to prevent the disclosure of information contained in its archives where such disclosure would be capable of interfering with the functioning and independence of that institution, in particular by jeopardising the performance of the tasks entrusted to it. That objective of protection shows that the archives so protected necessarily cover *any* document relating to the activities and tasks of the European institutions, of whatever date, of whatever type and in whenever medium which have been originated in or been received by the EU institutions or by their representatives in the performance of their duties, and which relate to the activities or performance of the tasks of those entities.[82] Moreover, Article 2 of the Protocol covers the archives of EU institutions, *whether located at the premises of the EU institution concerned or at other premises*[83], such as those of a service provider.

---

[80] See Annex to the EDPB-EDPS Joint Response to the LIBE Committee on the impact of the US Cloud Act on the European legal framework for personal data protection, available at https://edpb.europa.eu/sites/default/files/files/file2/edpb_edps_joint_response_us_cloudact_annex.pdf, page 8 [accessed 19 September 2022].

[81] Judgment of the Court of Justice of 17 December 2020, C-316/19, European Commission v. Republic of Slovenia, para 102 , ECLI:EU:C:2020:1030.

[82] Judgment of the Court of Justice of 17 December 2020, C-316/19, European Commission v. Republic of Slovenia, para 73-75, ECLI:EU:C:2020:1030.

[83] Judgment of the Court of Justice of 17 December 2020, C-316/19, European Commission v. Republic of Slovenia, para 78, ECLI:EU:C:2020:1030; Opinion of Advocate General of 3 September 2020 in Case C-316/19, para 49-50.

3.11. By way of example[84], with regard to the laws of the United States, in addition to **FISA 702**[85] applying to data kept by Cisco International Limited UK and Cisco Systems Inc. US[86], the reliance on the AWS data centres by Cisco Webex, including, as it appears, when the data is stored under the Webex Data Residency programme, **opens the possibility of the application of the US CLOUD Act**.[87] A request under the CLOUD Act directed to Cisco International Limited UK in particular, under the so-called "Data Access Agreement" between the US and the UK[88] might not be compatible with the Protocol absent the agreement of the Court or a decision by the EU judicature.

3.12. Hence, the EDPS considers that the Court, by migrating data to the data centres located in the EU has **partially complied with Condition 2. To fully comply with that condition the Court must still**:

(i) provide detailed information about the scope and application of the Cisco Webex Data Residency programme, in particular by identifying the effect of deployment of this programme, the personal data covered by it as well as the applicable level of data residency (global, limited, restricted)[89] per type of personal data**,**

(ii) clarify the notion of User Generated Data, in particular to explicitly include 'real time meeting data' in the category of User Generated Data, hence confirming that this data is covered by the Webex Data Residency,

(iii) demonstrate if, how and to what extent personal data covered by the Webex Data Residency programme prevents remote access (by sub-processors and third countries' authorities), to data stored and/or processed in the EU.

---

[84] The EDPS underlines that the legislation and practices of other countries of destination under the contractual clauses, such as India, raise difficulties in ensuring an essentially equivalent level of protection. See the study 'Government access to data in third countries' commissioned by the EDPB, accessible at https://edpb.europa.eu/system/files/2022-01/legalstudy_on_government_access_0.pdf. In particular, third country laws, e.g. India's, can also similarly to the United States, prohibit a data importer from informing the controller about disclosure requests, and provide for obligations on data importers to provide access to or to turn over data upon request, including cryptographic keys.

[85] Section 702 of the US Foreign Intelligence Surveillance Act of 1978 to establish a procedure for authorizing certain acquisitions of foreign intelligence, and for other purposes, as amended in 2008. (FISA), H.R. 6304 (50 U.S. Code §1881a). If data is stored by US companies (including EU subsidiaries) outside the United States, it may fall within the auspices of FISA 702.

[86] See para 3.30 of the EDPS Authorisation Decision of 31 August 2021.

[87] US Clarifying Lawful Overseas Use of Data Act (CLOUD Act), H.R. 4943.

[88] Agreement between the Government of the United States of America and the Government of the United Kingdom of Great Britain and Northern Ireland on Access to Electronic Data for the Purpose of Countering Serious Crime, in force since 3 October 2022, available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/836969/CS_USA_6.2019_Agreement_between_the_United_Kingdom_and_the_USA_on_Access_to_Electronic_Data_for_the_Purpose_of_Countering_Serious_Crime.pdf [accessed 26 October 2022].

[89] See point 2.16 of this Decision.

(iv) clarify if and to what extent transfers of personal data take place because of the Court's use of Cisco's Meeting Server, Private Meetings and Video Mesh.

### 3.1.3. Condition 3: Appropriate supplementary measures for TAC

3.13. In the EDPS Authorisation Decision of 31 August 2021, the EDPS requested 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 Court has carried 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 SDPCs for transfers under the GDPR as adapted to the Regulation. The Court should consider all examples of supplementary measures in Annex 2 of the EDPB Recommendations 01/2020, to identify which supplementary measures it would be necessary and appropriate to implement for transfers in the Court's use of Cisco Webex Meeting and related services.[90]

3.14. The EDPS notes that as part of the documentation provided to the EDPS on 1 September 2022, the Court did provide the TIA in Annex II to the Request for authorisation. Specifically, its Section B deals with the transfers of personal data that take place in the context of the Court's use of Cisco's TAC support services.

3.15. With regard to the data **transfers that take place in the context of TAC requests**, transfers of personal data in the provision of TAC services may fall under the use cases 6 and 7 of Annex 2 to the EDPB Recommendations 01/2020, where Cisco and other sub-processors providing these services may require access to data in the clear.[91]

3.16. The EDPS notes that although the Court did introduce contractual[92], organisational and technical supplementary measures,[93] as explained in Section 3.1.12 - **Condition 13**, it remains that **Cisco may have access to personal data** transferred in the context of TAC requests to recipients in the United States.[94]

3.17. In particular, the EDPS notes that **the Court did not fully comply with Conditions 12 and 13**, because it is unclear if it created a Single Point of Contact for TAC requests. Neither does the Court appear to anonymise or pseudonymise the case attachments, and manually provide Cisco with the minimum amount of data needed for the resolution of the problem.[95]

[90] Condition 3 of the EDPS Authorisation Decision of 31 August 2021.
[91] Point 3.68 of the EDPS Authorisation Decision of 31 August 2021.
[92] See Section 3.1.12 - Condition 13.
[93] Points 2.23 and 2.48 of this Decision.
[94] See Sections 3.1.11 - Condition 12 and 3.1.12 - Condition 13 of this Decision.
[95] See Sections 3.1.11 - Condition 12 and 3.1.12 - Condition 13 of this Decision.

3.18. Hence, the EDPS considers that the Court has **partially complied with Condition 3. To fully comply with that condition the Court must still**:

(i) comply with conditions identified under Sections 3.1.11 - **Condition 12**, 3.1.12 - **Condition 13**.

### 3.1.4. Condition 4: Adapted contractual clauses

3.19. In the EDPS Authorisation Decision of 31 August 2021, the EDPS requested that the new contractual clauses are concluded based on the model of the new standard data protection clauses ('SDPCs', also referred to as 'SCCs') for transfers under the GDPR adopted by the European Commission[96] 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.[97]

3.20. According to the information provided by the Court, the new set of contractual clauses are based on the model of the SDPCs for transfers under the GDPR adopted by the Commission on 4 June 2021.[98]

3.21. In the TIA, the Court specified that the contractual clauses were adapted to include, where relevant, references to the Regulation, identification of the EDPS as a supervising authority, and identification of the exclusive jurisdiction of the Court where cases are brought by a data subject against the Court.[99]

3.22. Module two of the SDPCs for transfers 'controller to processor' has been used for the drafting of the contractual clauses. Based on the EDPS assessment, these contractual clauses were complemented on the following points:

(i) Where appropriate, a reference to the Regulation and its 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 SDPCs as well as, in addition, a provision that these SDPCs 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. The same obligation shall also be applicable for any onward transfer

[96] 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 (Text with EEA relevance), OJ L 199, 7.6.2021, p. 31–61.
[97] Condition 4 of the EDPS Authorisation Decision of 31 August 2021.
[98] See footnote 93 of this Decision.
[99] Para 77 of the TIA.

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

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

3.23. The EDPS **welcomes the inclusion of contractual clauses based on the SDPCs**. However, considering the role of the Court as public authority carrying out its tasks in the public interest under EU law, the contractual clauses **need to be further adapted to the specific requirements of the Regulation** to ensure an essentially equivalent level of protection and that the Court remain in control of the whole processing. **The contractual clauses based on the SDPCs for transfers under the GDPR need to be completed** as follows:

(i) Clause 8(2) on the principle of purpose limitation needs to reflect that transfers can take place solely to allow tasks within the competence of the Court to be carried out under EU law.[100]

(ii) Clause 8(8) (last sentence) sets out that onward transfers are subject to compliance by the data importer with all other safeguards under the Clauses, in particular purpose limitation. Clause 9(b) foresees that the data importer shall enter into binding commitment with sub-processors including the same data protection obligations as provided by the Clauses. Clause 8(8) should also reflect that transfers from the Court can take place solely to allow tasks within the competence of the Court to be carried out under EU law.[101] Onward transfers should only be possible if they are necessary for the fulfilment of the mandate of the Court and are justified by an important reason of public interest as recognised by EU law. In addition, for compliance with all other safeguards of the Clauses particular attention should be paid for purpose limitation and data minimisation.

(iii) As regards the use of sub-processors, Clause 9(a) reads: '*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*

[100] Article 47(1) of the Regulation. The EDPS is of the view that this requirement also applies to appropriate safeguards under Article 48 of the Regulation, having regard in particular to the standard of essential equivalence that has to be ensured for transfers based on appropriate safeguards, in accordance with the Schrems II judgment, in particular paras 95-96 (Judgment of the Court (Grand Chamber) of 16 July 2020, C-311/18, Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems, ECLI:EU:C:2020:559).

[101] Article 47(1) of the Regulation. The EDPS is of the view that this condition applies to onward transfers stemming from transfers based on Article 48 of the Regulation (appropriate safeguards), having regard in particular to Article 45 that expressly covers onward transfers.

*provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.*' The EDPS considers that the clauses should provide for meaningful time to assess and object to the use of a given sub-processor. Therefore, Clause 9(a) should delete the wording 'or as early as practically possible *(if so)*' since they can be interpreted as lifting Cisco's obligation to inform the Court at least one month in advance.

(iv) Concerning the assessment of local laws and practices affecting compliance with the clauses[102] the parties must take into account Privileges and Immunities of the Court based on Article 2 of Protocol VII of the Treaty on the Functioning of the European Union[103]. In particular it should be assessed, to what extent these privileges and immunities are recognized in the legal framework of the importer or of the sub-processors.

(v) Clause 14 reads: '*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.'* In case of restrictions, since the Court is subject only to the Regulation, the clauses should refer only to Article 25 of the Regulation. It should also be made clear that restrictions under Article 25 of the Regulation may only be imposed by the Court.

(vi) In case of access requests by public authorities, Clause 15 must be aligned with the conditions under Section 3.1.8 - **Condition 9**.

(vii) Clause 16 should provide that not only the data importer but also its sub-processors should promptly notify the data exporter if they are unable to comply with the clauses.

(viii) Concerning Clause 17, the EDPS recommends that, in line with the practices of the DG BUDG of the European Commission for service contracts, the application of the law of the Member State where the EUI is established should be complementary to the application of EU law.

---

[102] For more information on how to conduct such assessment, see Recommendations 2/2020 on the European Essential Guarantees for surveillance measures of the European Data Protection Board, available at https://edpb.europa.eu/sites/default/files/files/file1/edpb_recommendations_202002_europeanessentialguaranteessurveillance_en.pdf [accessed 30 September 2022].

[103] Consolidated version of the Treaty on the Functioning of the European Union, Protocol (No 7) on the privileges and immunities of the European Union, OJ C 326, 26.10.2012, p. 266–272.

(ix) Finally, the contractual clauses refer to Annexes 1a and 1b (description of the transfers) as being an integral part of the clauses,[104] whereas Exhibit B (list of sub-processors authorised by the Court) and Exhibit C (Information security)[105] to the Supplementary Agreement are not. As Exhibits B and C should also be binding on Cisco Systems, Inc. as signing party of the contractual clauses, these should also form an integral part of the clauses.

3.24. Hence, the EDPS considers that the Court **has partially complied with Condition 4. To fully comply with that condition the Court must still:**

a) further adapt the contractual clauses as follows:

(i) Clause 8(2) (Purpose limitation) and Clause 8(8). (onward transfers): must reflect that transfers can take place 'solely to allow tasks within the competence of the Court to be carried out under EU law';

(ii) Clause 8(8) (onward transfers) must refer to compliance with the principle of data minimization;

(iii) Clause 9(a) (Use of sub-processors) must delete 'or as early as practically possible *(if so)*';

(iv) Clause 14 (Local laws and practices affecting compliance with the Clauses) must only refer to restrictions under Article 25 of the Regulation and they may only be imposed by the Court;

(v) Clause 15 (Obligations of the data importer in case of access by public authorities): *See below* ***Condition 9*** *on disclosure requests*;

(vi) Clause 16 (Non-compliance with the Clauses and termination) must provide that not only the data importer but also its sub-processors should promptly notify the data exporter if they are unable to comply with the clauses;

(vii) Clarify that Exhibits B and C also form an integral part of the contractual clauses,

b) assess to what extent the Privileges and Immunities of the Court based on Article 2 of Protocol VII of the Treaty on the Functioning of the European Union[106] are recognized in the legal framework of Cisco Systems Inc. US or of its sub-processors.

[104] See page 7 of the Supplementary Agreement.
[105] Clause 9(a) and (f) of the contractual clauses.

### 3.1.5. Condition 5: Docking clause

3.25. In the Authorisation Decision of 31 August 2021, the EDPS found that the Court concluded the initial contract with Cisco International Limited UK and a number of its annexes with Cisco Systems Inc. US. However, it appeared unclear how the provisions of the contract, in particular those relating to transfers, bind other Cisco establishments (e.g. Cisco Systems Inc. US or Cisco Mexico), its affiliates, partners and sub-processors. Annexes to the contract (which originate with Cisco) set out that references to "Cisco" mean Cisco Systems Inc. or its applicable affiliates.[107]

3.26. Hence, the EDPS required that the Court concludes the new contractual clauses with Cisco International Limited UK and Cisco Systems Inc. US for controller to processor transfers (from the Court 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 Court's use of Cisco Webex Meeting and related services to adhere to the new contractual clauses concluded by the Court.[108]

3.27. Regarding the new SDPCs between a controller and processor, the EDPS notes that the current draft of the Supplementary Agreement is to be signed between the Court and Cisco International Limited UK (named as a Supplier), while the contractual clauses, constituting Exhibit A to that Agreement, between the Court and Cisco Systems Inc. US (named as a processor).

3.28. Article 1(4)(d) of the Supplementary Agreement deleted Article 11(2) of the contract and added the new clause (Art. 11(2)(d)), which reads: [f]*or clarity, the Supplier* [Cisco International Limited UK] *agrees that Exhibit A and its Annexes below, are an integral part of the Agreement and its Amendment. Any obligation on the Processor* [Cisco Systems Inc. US], *as identified in Exhibit A below, is part of the contractual obligations of the Supplier under the Agreement.*

3.29. Although the contractual clauses are to be signed with Cisco Systems Inc. US, **any obligations of Cisco Systems Inc. US under the contractual clauses also bind Cisco International Limited UK**.

3.30. Regarding the processors to processor transfers, the EDPS notes that Clause 9(f) of the contractual clauses reads: [t]*he use of sub-processors is, in case of any onward transfer of personal data, subject to a contract being signed between the data importer* [Cisco Systems Inc. US] *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*

[107] Point 3.19 of the Authorisation Decision of 31 August 2021.
[108] Condition 5 of the Authorisation Decision of 31 August 2021.

*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.*' Further, Clause 9(g) reads that: '[p]*aragraph (f) also applies in case of an onward transfer of personal data to any affiliate or partner of the data importer* [Cisco Systems Inc. US] *or a sub-processor.*'

3.31. Combined with Cisco International Limited UK's acceptance of the obligations stemming from the contractual clauses, as well as Clauses 9(f) and (g), the **EDPS considers that these provisions offer sufficient contractual guarantees** that any onward transfer will respect the level of protection of natural persons guaranteed by the Regulation, **subject to** the EDPS' further conditions listed in Section 3.1.4 - **Condition 4**.

3.32. Regarding the possibility of other recipients adhering to the contractual clauses, the EDPS notes that Clause 7 of the contractual clauses **contains a docking clause to this end**. The Clause reads that: '[a]*n 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.*' The Clause further reads that '[o]*nce 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.*' and that '[t]*he acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.*'

3.33. Considering the above, the EDPS considers that the Court has **complied with Condition 5**.

### 3.1.6. Condition 6: Binding effect of the contractual clauses

3.34. In the Authorisation Decision of 31 August 2021, the EDPS required that the Court ensures that the provisions of the new contractual clauses, including those in the main body of the contract, apply to and are binding upon other Cisco establishments (e.g. Cisco Systems 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).[109]

3.35. Based on the analysis of the Supplementary Agreement, together with the contractual clauses, it is clear that the provisions of **the new contractual clauses do not automatically apply to nor are binding upon** other Cisco establishments, its affiliates, partners and sub-processors. Rather, under Clause 7 of the contractual

[109] Condition 6 of the Authorisation Decision of 31 August 2021.

clauses[110], these Cisco entities have the right to accede to these SSCs, subject to the agreement of the Court and Cisco Systems Inc. US.

3.36. Even though this accession to the contractual clauses is not automatic, the Supplementary Agreement **contains other guarantees** that ensure that the same level of protection of the data is maintained when either Cisco Systems Limited US or Cisco International Limited UK engages a sub-processor.

3.37. Clause 9(b) of the SDPCs on the use of sub-processors reads that: [w]*here the data importer* [Cisco Systems Limited US] *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* [...]'.

3.38. Furthermore, Article 1(4)(c) of the Supplementary Agreement reads that: '[i]*f part or all of the processing of personal data is subcontracted to a third party, the Supplier* [Cisco International Limited UK] *shall pass on the essentially equivalent obligations regarding data protection in writing to those parties, including subcontractors. At the request of the Customer, the Supplier shall provide a document providing evidence of this commitment.*' What is more, under Article 1(4)(c) of the Supplementary Agreement, Clause 9 of the contractual clauses *'applies to the use of sub-processors by the Supplier* [Cisco International Limited UK]*, where it involves a transfer 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.*'

3.39. However, the EDPS recalls that, where the accession to the contractual clauses is not automatic for all Cisco entities, **the Court must ensure that the SDPCs under the GDPR which are the basis for onward transfers between the processors include additional provisions to align them with the specific context of the Regulation**. Namely, the Court should add parallel additional contractual provisions as these that must be included in the contractual clauses under Section 3.1.4 - **Condition 4**. This is to ensure that the processing of transferred data meets the requirements of EUDPR and ensure equivalent level of protection guaranteed by EUDPR, as well as to ensure that the EUI remains in control of the whole processing and any transfers.

3.40. Next, under Clause 9(f) of the contractual clauses, the SDPCs between Cisco International Limited UK[111] or Cisco Systems Inc. US and their sub-processors prevail over any other contractual obligation between these Cisco entities and the sub-processors. In addition, this Clause applies '*in case of an onward transfer of personal data to any affiliate or partner of the data importer* [Cisco Systems Inc. US or Cisco International Limited UK[112]] *or a sub-processor*' (Clause 9(g)).

[110] See point 3.32 of this Decision.
[111] Clause 9 of the contractual clauses applies on the basis of Art. 1(4)(c) of the Supplementary Agreement.
[112] Clause 9 of the contractual clauses applies on the basis of Art. 1(4)(c) of the Supplementary Agreement.

3.41. Hence, the EDPS considers that the Court has **complied with Condition 6**.

### 3.1.7. Conditions 7 and 8: Sufficient guarantees from all the recipients

3.42. In the Authorisation Decision of 31 August 2021, the EDPS required that the new clauses must 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.[113]

3.43. Further, the EDPS required that if the other recipients do not adhere to the new contractual clauses concluded by the Court, the Court needs to obtain 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 Court has 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 Court during the TIA.[114]

3.44. As mentioned above (Section 3.1.6 - **Condition 6**), the new contractual clauses are binding on Cisco entities, its affiliates and other sub-processors. These clauses include Annexes 1a and 1b, which describe the remaining transfers of personal data and applicable measures associated to the use of Cisco Webex Meetings and TAC support information, respectively. Both exhibits include a description of the remaining transfers, i.e.: the categories of data subjects whose personal data is transferred; the categories of personal data transferred; the sensitive data transferred; the frequency of the transfers; the nature of the processing, including a description of specific technical and organisational measures implemented to secure personal data; the purposes of the data transfer and further processing; the retention period; a reference to Exhibit B as regards the list of sub-processors. Exhibit B describes, for each sub-processor, the personal data processed, the service type and purpose of processing, the location of the data and the official address of the sub-processor. Moreover, Annexes 1a and 1b refer to the EDPS as the supervisory authority and include additional technical and organisational commitments from the data importer.

3.45. Hence, the EDPS considers that the Court has **complied with Condition 7**.

3.46. As already mentioned (Section 3.1.6 - **Condition 6**), for recipients that do not adhere automatically to the contractual clauses, essentially equivalent obligations shall be passed on any sub-processor, including any affiliate or partner of Cisco, and the latter shall apply technical and organisational measures that, at least, reach the

[113] Condition 7 of the Authorisation Decision of 31 August 2021.
[114] Condition 8 of the Authorisation Decision of 31 August 2021.

same level of security as those mentioned in Exhibit C of the Supplementary Agreement (Clause 9(f) and (g) of the contractual clauses).

3.47. As to whether the measures implemented for transfers to other recipients correspond to the role of the recipients in the processing of transferred data the recipient will carry out, the **EDPS notes a discrepancy** between the TIA and Exhibits B (List of sub-processors) and D (Privacy Data Sheets). The latter include WalkMe Inc. and Vbrick as sub-processors for Webex meeting services whereas the TIA indicates that the Court:

- turned off the feature (guidance on how to use Webex online) that would involve transfers to Walkme Inc.[115], and

- only has a license to organise Webex meetings up to 1 000 participants, knowing that Vbrick is implicated only to provide capacity for over 3 000 participants[116].

3.48. As to whether the measures implemented for transfers to other recipients are in line with the assessments made and supplementary measures identified by the Court in the TIA, the EDPS notes that Clause 9(f) of the contractual clauses refers to the SDPCs adopted by the Commission based on Article 46(2)(c) requiring that the sub-processor shall apply technical and organisational measures that at least reach the level of measures listed in Exhibit C (Information Security Exhibit). However, **Exhibit C contains general security measures and does not refer to the supplementary measures identified in the TIA** and reflected in Annexes 1a and 1b of the contractual clauses.

3.49. Hence, the EDPS considers that the Court has **partially complied with Condition 8. To fully comply with that condition the Court must still**:

(i) revise the list of sub-processors and removes those that are not actually involved in the processing, and

(ii) specify that any sub-processor should be subject to a contract including the appropriate SDPCs adopted by the Commission as well as to appropriate supplementary measures included in the SDPCs to be tailored depending on the role of the sub-processor in the processing activity.

### 3.1.8. Condition 9: Obligation to notify, redirect and challenge disclosure requests

3.50. In the Authorisation Decision of 31 August 2021, the EDPS requested that the new contractual clauses contain clear obligations and binding commitments from Cisco to notify and redirect to the Court any disclosure requests for Court's data that

[115] Para 47 of the TIA.
[116] Paras 48-50 of the TIA.

Cisco, its affiliates or its sub-processors receive and to legally challenge such disclosure requests.[117]

3.51. Clause 15 of the contractual clauses signed between the Court and Cisco Systems Inc. US reproduces the respective clause from the SDPCs adopted by the Commission under the GDPR.[118]

3.52. As already emphasised in the EDPS Authorisation Decision of 31 August 2021, the **Court is subject to Protocol (No 7) to the Treaties on the privileges and immunities of the European Union, including as regards the inviolability of archives**, which includes personal data held on behalf of the Court in the premises of Cisco establishments, its affiliates, partners and sub-processors.[119] The EDPS continues to consider that the respect of the privileges and immunities of the EUIs, as recognised in the Treaties, and where extended to an EUI by a third country, in particular e.g. the inviolability of the EUI's archives, contributes to the protection of personal data that EUIs process or that is processed on EUIs' behalf in the EU and outside the EU. However, the EDPS has already had the opportunity to also emphasise to the EUIs, at the occasion of an investigation into EUIs' use of services of another US service provider, that the EUIs had few guarantees under their contract with that provider to be actually in a position to defend their privileges and immunities against disclosure requests from third-country governments and processors subject to their jurisdiction.[120] This was contrary to Articles 4(1)(f) and 49 of the Regulation. Where the obligations and contractually binding commitments from Cisco may be rendered ineffective because the national legislation in the third country prevents disclosure of the requests or substantial information thereof, Cisco must inform the Court of its inability to comply with the Supplementary Agreement and/or the Contractual Clauses, thus offering the Court the option to suspend the transfers.[121]

3.53. As already explained,[122] the contractual clauses **need to be further adapted to the specific requirements applicable to Union institutions and bodies as provided for by the Regulation** to ensure an essentially equivalent level of protection and that the Court remain in control of the whole processing.[123] Clause

[117] Condition 9 of the EDPS Authorisation Decision of 31 August 2021.
[118] See Section 3.1.4 of this Decision.
[119] See point 3.10 of this Decision and references to case law therein.
[120] See EDPS Public Paper on Outcome of own-initiative investigation into EU institutions' use of Microsoft products and services, available at https://edps.europa.eu/sites/edp/files/publication/20-07-02_edps_euis_microsoft_contract_investigation_en.html#unauthorised-disclosure [accessed 26 October 2022].
[121] See Recital 67 of the Regulation and Judgment of the Court (Grand Chamber) of 16 July 2020, C-311/18, Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems, ECLI:EU:C:2020:559, para 142 and EDPB Recommendations 01/2020, para 134.
[122] Points 3.10 and 3.23 of this Decision.
[123] The lack of control generated by transfers is notably illustrated in Recital 71 of the Regulation: '*When personal data moves across borders outside the Union it may put at increased risk the ability of natural persons to*

15 of the contractual clauses should include an obligation for Cisco to, simultaneously, a) **notify to the Court**, b) **redirect to the Court and seek the instructions from the Court,** and c) **challenge** any disclosure requests it receives. These obligations **should concern *any* requests** for disclosure. In addition, these obligations to notify, redirect and challenge, should be carried out **independently of one another**, i.e., not only where one of the obligations cannot be fulfilled.

3.54. In addition, the EDPS notes that Art. 1(4)(c) of the Supplementary Agreement signed between the Court and Cisco International Limited UK contains obligations regarding the disclosure requests that do not fully replicate the ones included in the contractual clauses.[124] In particular, it would seem that the obligation to challenge a request for disclosure would be applicable only where the local laws prohibit to notify the data exporter (the Court) of such request. The obligation to challenge in the contractual clauses are not dependent upon the existence of a prohibition to notify.

3.55. Furthermore, under Conditions 5 and 6 of the EDPS Authorisation Decision of 31 August 2021, the obligations of Cisco International Limited UK should be the same as those of Cisco Systems Inc. US under the contractual clauses.[125] It is still not clear, having regard to the drafting of Article 1(4)(d)[126] of the Supplementary Agreement concluded with Cisco International limited UK whether also CISCO US is also bound by the Supplementary Agreement, The Court must hence remove the uncertainty stemming from the current wording of the mentioned provisions.

3.56. Hence, the EDPS considers that the Court has **partially complied with Condition 9. To fully comply with that condition the Court must still**:

---

*exercise data protection rights, in particular to protect themselves from the unlawful use or disclosure of that information. At the same time, national supervisory authorities and the European Data Protection Supervisor can be unable to pursue complaints or conduct investigations relating to the activities outside their jurisdiction.*'

[124] Art.1(4)(c) of the Supplementary Agreement between the Court and Cisco International Limited UK provides that: '[w]*ithout 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*' (emphasis added).

[125] See point 3.29 of this Decision.

[126] Art. 1(4)(d) of the Supplementary Agreement between the Court and Cisco International Limited UK provides that: *"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."*

(i) include an obligation for Cisco (including its sub-processors) to notify any disclosure requests it receives to the Court at default and as a self-standing obligation;

(ii) include an obligation for Cisco (including its sub-processors) to redirect any disclosure requests to the Court and seek the instructions from the Court at default and as a self-standing obligation;

(iii) include an obligation for Cisco (including its sub-processors) to introduce a legal challenge against any access request at default and as a self-standing obligation; and

(iv) ensure that the obligations of Cisco International Limited UK correspond to those of Cisco Systems Inc. US under the contractual clauses.

### 3.1.9. Condition 10: No back door policy

3.57. In the Authorisation Decision of 31 August 2021, the EDPS requested that the new 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) 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.[127]

3.58. The Court informed the EDPS that specific clauses were added in the Supplementary Agreement to address this Condition.

3.59. Article 1(4) of the Supplementary Agreement deleted Article 11(2) of the contract and added the new clause (Art. 11(2)(c)), which is also inserted in Exhibit A of the contract ( contractual clauses), Annexes 1a and 1b, Sections C, Point 1.

3.60. The clause added to contractual clauses reads[128]: '*[t]he data importer 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;*

[127] Condition 10 of the EDPS Authorisation Decision of 31 August 2021.
[128] A clause of the same wording, but different formatting is added in Art. 1(4) of the Supplementary Agreement.

*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.'*

3.61. In the first place, the EDPS welcomes that the inclusion of this new clause in the Supplementary Agreement and its Exhibits creates a contractual obligation and is a legally binding commitment for the parties.[129]

3.62. In the second place, the EDPS notes the new clause in the Supplementary Agreement and its Exhibits partially addresses Condition 10. The new clause gives effect to letter i) and ii) of the Condition, where Cisco sufficiently certifies that it has not purposefully created back doors or similar programming that could be used to access the system and/or personal data, and that it has not purposefully created or changed its business processes in a manner that facilitates access to personal data or systems.

3.63. However, the new clause in the Supplementary Agreement and its **Exhibits does not give effect to letter iii) of the Condition**, where Cisco was required to certify 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.

3.64. The EDPS notes that, without giving effect to letter iii) of the Condition, the new wording of the clause does not fully guarantee its effectiveness.[130] While Cisco indeed certified that it did not purposefully created back doors or similar programming nor created or changed business processes, Cisco did not certify that it is not obliged by law applicable to it to do so. This leaves the uncertainty that Cisco is in fact already obliged to create or maintain back doors or to facilitate access to personal data or systems or for Cisco to be in possession or to hand over the encryption key. Hence, without this assurance from Cisco, the binding effect of the entirety of the new clause is undermined.

3.65. The EDPS therefore considers that the Court has **partially complied with Condition 10. To fully comply with that condition the Court must still**:

- ensure that Cisco certifies 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.

[129] Following the EDPS recommendation in the Authorisation Decision of 31 August 2021, point 3.46.
[130] See paragraph 110 of the EDPB Recommendations 01/2020.

### 3.1.10. Condition 11: End-to-end encryption of videoconferencing communications

3.66. In the Authorisation Decision of 31 August 2021, the EDPS requested that the new contractual clauses must ensure that the technical supplementary measures of the use cases 1 and 3 of Annex 2 to the EDPB recommendations 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.[131] In the TIA, the Court explained that it uses two types of encryption as technical supplementary measures - encryption of data in transit and the newly-deployed (end of August 2021) Zero Trust Security End-to-End encryption.[132]

3.67. In the TIA, the Court explained **data in transit is encrypted** in communications between cloud registered Webex Apps, Webex Room devices and Webex servers.[133] The Court stated that Cisco Webex uses *'TLS protocol with version 1.2 or later with high strength cipher suites* [...]' for call signalling, as well as the use of UDP protocol to carry all media streams over the TLS channel, where *'media packets are encrypted using either AES 256 or AES 128 based ciphers* [...]'.[134]

3.68. Next, the Court explained that the so-called **Webex Zero Trust Security End-to-End encryption** is enforced when a user at the CJEU organises a videoconference.[135] The Court explained that "[t]*he 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.*"[136]

3.69. In order to provide a more detailed description of the Zero Trust End-to-End encryption, the Court referred to the Zero-Trust Security for Webex White Paper[137], **which the EDPS had already analysed** in the context of the original EDPS Authorisation Decision of 31 August 2021.[138]

3.70. Based on the mentioned White Paper and as already mentioned in the EDPS Authorisation Decision of 31 August 2021[139], the solution leverages the Messaging Layer Security (MLS), which is meant to generate and manage a key shared among the meeting participants and ensure that the only individuals who can decrypt the media are the ones who are in the meeting. The Webex Zero Trust Security End-to-

[131] Condition 11 of the EDPS Authorisation Decision of 31 August 2021.
[132] Section V.A. of the TIA.
[133] Paras 84-90 of the TIA.
[134] Paras 84-88 of the TIA.
[135] Para 93 of the TIA.
[136] Paras 92-93 of the TIA.
[137] Zero-Trust Security for Webex White Paper, accessible at https://www.cisco.com/c/en/us/solutions/collateral/collaboration/white-paper-c11-744553.html [accessed 23 September 2022].
[138] Point 3.51 of the EDPS Authorisation Decision of 31 August 2021.
[139] Point 3.51 of the EDPS Authorisation Decision of 31 August 2021.

End solution also integrates an 'end-to-end verified identity' feature that ensures that, inter alia, Cisco cannot impersonate a participant and thus be able to decrypt the exchanges. However, the EDPS notes that the Court has not provided detailed information on how the end-to-end identity verification had been implemented in the Court's use of Cisco services.

3.71. As already expressed in the EDPS Authorisation Decision of 31 August 2021, if certain conditions therein expressed are met,[140] the EDPS considers that, with regard to the services to which Webex Zero Trust Security End-to-End solution applies, that solution covers the requirements for use cases 1 and 3 of Annex 2 to the EDPB Recommendations 1/2020, hence constitutes an effective measure against unauthorized disclosure of personal data caused by access resulting from the application of third country laws.

3.72. Nevertheless, the EDPS underlines that the use of the Webex Zero Trust Security End-to-End solution is **still not possible in some circumstances**. These circumstances do not appear to have changed from those already known and taken into account in the EDPS Authorisation Decision of 31 August 2021.[141] Specifically, for the Webex Zero Trust Security End-to-End solution to work, the meeting participants must use the Webex App[142] or cloud registered Webex devices. In addition, the solution cannot be used, inter alia, for video-device enabled meetings, Linux clients, or Network-Based Recording.[143]

3.73. Hence, on the day of issuing this present Decision, the EDPS understands that Cisco had not yet deployed the publicly promised 'ubiquitous E2E security' for every Webex meeting, i.e. covering every endpoint that can join a Webex meeting.[144] It is the EDPS' understanding that Cisco had neither provided the Court with a timeline of when this deployment is planned to take place.

3.74. The EDPS notes that where the Webex Zero Trust Security End-to-End solution does not apply as explained in point 3.72 above, the technical measure in place is the encryption in transit[145] which is applied under the control of Cisco. This is the case for instance during the usage of Webex media nodes, built over AWS software and infrastructure, which enable the call signalling and real time exchanges, or when a user connects to a Webex meeting using a device unable to use the Webex Zero Trust Security End-to-End encryption. Hence, the EDPS considers that encryption in transit provides confidentiality against third parties (such as AWS, ISPs, etc.) that have access to the communication streams as well as against other external threats.

---

[140] Point 3.56 of the EDPS Authorisation Decision of 31 August 2021.
[141] Point 3.52 of the EDPS Authorisation Decision of 31 August 2021.
[142] The Court calls 'Webex App' the software installed in the Court's computers. Cisco had a different language in the White paper describing the Webex Zero Trust Security End-to-End solution (see footnote 137) and seems to call 'Webex App' the Webex mobile app and **not** the Webex Meetings client SW.
[143] Pages 23-24 of Annex 1a to Exhibit A.
[144] Point 3.52 of the EDPS Authorisation Decision of 31 August 2021. See also: Zero-Trust Security for Webex White Paper, accessible at https://www.cisco.com/c/en/us/solutions/collateral/collaboration/white-paper-c11-744553.html [accessed 23 September 2022].
[145] Point 3.67 of this Decision.

However, because the encryption keys are known to Cisco, since they are generated by a Cisco-controlled software, **encryption in transit still allows** the possibility for Cisco **to access the data**, including based on a request for access resulting from the application of third country laws.

3.75. The EDPS takes note of the organisational measures that the Court will implement to deal with situations where the use of Webex Zero Trust Security End-to-End encryption is not possible. In such circumstances, the Court committed itself to either use alternative solutions (such as Cisco Meeting Server for internal meetings) or evaluate the level of protection required for the specific meeting (for example in the case of public or semi-public meeting).[146] In addition, the Court claims to have taken organisational measures to limit the situation where Webex Zero Trust Security End-to-End encryption is not possible by equipping its own meeting rooms with infrastructure compatible with Webex Zero Trust Security End-to-End encryption and by blocking the possibility to call in a meeting by phone. The Court also commits to informing the external users before the meetings, where necessary, about the technical requirements needed for the proper use of Webex Zero Trust Security End-to-End encryption.[147]

3.76. The EDPS **welcomes the organisational measures** implemented by the Court and recognises that they can indeed **limit** the instances where the Webex Zero Trust Security End-to-End encryption is not available for videoconferencing communications. In that regard, the combination of technical measures - the use of Webex Zero Trust Security - and the organisational measures planned will contribute to strengthening the overall level of protection of personal data. However, in line with his previous conditions and with the principle of data minimisation, the EDPS maintains that the Court must continue seeking that the state of the art end-to-end encryption technology in line with the technical requirements of the use cases 1 and 3 of Annex 2 to the EDPB recommendations is adopted for ***all the Webex videoconferencing communications***.

3.77. The EDPS advises that the Court liaise with Cisco to encourage it **to extend as soon as possible the Zero Trust End-to-End Encryption feature to as many devices as possible**, thus reducing the need for organisational measures and offer this opportunity to a wider audience. In addition, the Court must ensure that the use of the organisational measures proposed are monitored regularly as to their implementation and effectiveness, and enforced in accordance with the Court internal regulations.

3.78. Hence, the EDPS considers that the Court has **partially complied with Condition 11. To fully comply with that condition the Court must still:**

(i) continue seeking that state of the art end-to-end encryption technology in line with the technical requirements of the use cases 1 and 3 of Annex 2 to the EDPB

[146] Para 96 of the TIA.
[147] Para 97 of the TIA.

recommendations is adopted for all the Webex videoconferencing communications, without exceptions, unless the Court does not plan to use those devices that are not compatible with such technical requirements in any of its communications, independently from the level of risk for data subjects involved. Where the Zero Trust End-to-End Encryption is used, it has to be deployed for all usages, without a risk based approach;

(ii) provide the EDPS with more detail on the organisational measures aimed at preventing that devices that are not compatible with said technical requirements are used, including on monitoring and enforcing procedures to ensure the effective use of the planned organisational measures.

### 3.1.11. Condition 12: Pseudonymisation or combination of measures to prevent access

3.79. In the Authorisation Decision of 31 August 2021, the EDPS requested that the new contractual clauses must ensure 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.

3.80. In the first place, the EDPS notes that neither the Supplementary Agreement nor the TIA provided by the Court appear to **not contain any information related to the application of state of the art pseudonymisation technologies** in the context of the Court's use of Cisco Webex and related services. The EDPS notes that the only instance where pseudonymisation is applied is with the use of the Unique User ID (UUID) identifier, which however was already provided intrinsically by the Cisco system before the adoption of the EDPS Authorisation Decision of 31 August 2021.

3.81. Simultaneously, as analysed in Section 3.1.10 - **Condition 11**, the EDPS considers that while the deployment of the Zero Trust Security End-to-End solution encryption **has brought a significant improvement by limiting Cisco's access to the real time meeting data (video, voice, chat)**, Cisco **maintains the capacity to access personal data** processed, especially where exceptions to that solution apply, as well as to User and Host and Usage Information.[148]

3.82. In the second place, the EDPS takes note that that the Court applied some technical and organisational measures aimed at preventing Cisco from having access to data, as also mentioned in points 1.41-1.56 and Section 3.1.10 - Condition 13.

[148] Points 2.20 of this Decision, and para 14 of the TIA.

3.83. Regarding the transmission of User Information, the Court employs the use of an Identity Provider technical solution (F5) operating under their control, aiming to control the information that is transmitted to Cisco when internal users are authenticated, via the SAML protocol.[149] The EDPS understands that with this technical measure the registration of the users of the Court takes place under the control of the Court, while the transmitted information when users are to be authenticated by Cisco consists of the username and email address, avoiding the transmission of phone numbers and other organisational information of the user. Nevertheless, the EDPS notes that the **Court did not provide clear information** on:

(i) whether for internal users the username is a pseudonymous identifier not leading to the identification of natural identifiers such as first and/or last name, whereas it states that 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*' (emphasis added)[150];

(ii) the necessity and purpose of e-mail addresses of internal users, whereas it states that '[t]*he CJEU will not require **external users** to provide the e-mail addresses, phone numbers or room device information when joining a meeting'* (emphasis added)[151].

3.84. Regarding Host and Usage Information of internal users, the EDPS understands that the Court applies another technical solution at a network level, aiming to protect the IP addresses of the devices of the Court users, when they are connected to Cisco either from the local network, or from remote places through the VPN.[152] This technical solution only transmits the Public IP address of the Court, instead of the IP address of the device of the users, and other IP addresses of network equipment along the path of the network connection between the user and Cisco Cloud services.

3.85. Regarding TAC Support Information and Customer Case Attachment Information, the EDPS notes that the Court applied organisational measures in order to limit the transmission of personal data.[153] Notably:

- the Court informed that '[w]*hen 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)*.'[154] However, as also explained in

[149] See point 2.47 of this Decision.
[150] Para 128 of the TIA.
[151] Para 128 of the TIA.
[152] See point 2.37 of this Decision.
[153] See Section 3.1.12 - Condition 13, and points 2.35-2.48 of this Decision.
[154] Para 139 of the TIA.

point 3.97, it **remains unclear if the personal data of the 'helpdesk' staff will be transmitted to Cisco or if functional non-personal contact data will be used**. It is also **unclear if the staff of the 'helpdesk' will anonymise the data coming from the end users' requests for technical assistance**;

- the Court stated that, to avoid transfers of personal data, despite making use of the 'follow the sun' policy, the Court will open a support case during EU business hours, so that the case is dealt '*initially*' by CISCO '*entities*' in EU.[155] The EDPS notes that this measure **does not exclude the likely possibility that some support cases will be dealt with by non-EU entities**, hence involving transfers, **and invites the Court to clarify this issue**;

- the Court stated that it will adopt internal policies with '*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*'[156]. The EDPS notes that while such organisational measures are good internal practices contributing to the minimisation of personal data in support request, they **do not completely avoid the presence of personal data within the support records. Furthermore, once personal data are stored in the US, no request for deletion from the Court will be able to be effective against the possibility of Cisco to access and store the data before the deletion request, if so instructed by applicable national law.**

3.86. The EDPS notes that the Court did not report any measures to avoid that logs of the processing of "static" content by Akamai Technologies Inc. content delivery network be transferred to the US or that any effective supplementary measure was adopted.

3.87. The EDPS notes that the Court did not report any measures to avoid that logs of the Hybrid Calendar Services, which also contains user identifiers (UUID), be accessible by Cisco.

3.88. Considering the above, the **EDPS takes the view that the implemented supplementary measures applicable to transfers that still take place do not effectively prevent Cisco in all cases from having access to personal data**.

3.89. Hence, the EDPS considers that the Court has **partially complied with Condition 12. To fully comply with that condition the Court must still**:

(i) implement conditions identified under Sections 3.1.2 - **Condition 2,** Section 3.1.10 - **Condition 11** and Section 3.1.12 - **Condition 13**.

### 3.1.12. Condition 13: No access to personal data

3.90. In the Authorisation Decision of 31 August 2021, the EDPS requested that the new contractual clauses include clear obligations and commitments that:

[155] Para 140 of the TIA.
[156] Para 142 of the TIA.

(i) by default Cisco does not have access to the Court data;

(ii) Cisco will provide remote technical assistance, only in case a Single Point of Contact (SPoC) from the Court makes a formal request, and in that case the Court will provide manually the minimum amount of anonymised 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 Court SPoC, Cisco shall not have access to other Court data.

3.91. The Court informed the EDPS that specific clauses were added in the Supplementary Agreement to address this Condition.

3.92. Article 1(4) of the Supplementary Agreement deleted Article 11(2) of the contract and added the new clause (Art. 11(2)(c)), which is also inserted in Exhibit A of the contract ( contractual clauses), Annexes 1a and 1b, Sections C, Point 2.

3.93. The clause added to contractual clauses reads[157]: '[t]*he 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.*'

3.94. In addition, the last sentence of Art. 1(4) of the Supplementary Agreement reads that: '*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.*'

3.95. In the first place, the EDPS notes that the inclusion of this new clause in the Supplementary Agreement and its Exhibits creates a contractual obligation and is legally binding commitment for the parties.[158]

3.96. In the second place, the EDPS considers that the new clause is in line with the requirements of Condition 14 as it includes clear obligations and commitments from Cisco regarding access control. In addition, the last sentence of Art. 1(4)(c) of the Supplementary Agreement, contractually binds Cisco that anything in Exhibit D, i.e., the Data Privacy Sheets, that is not compatible with these obligations, do not apply to the processing of personal data by Cisco.

[157] A clause of the same wording, but different formatting is added in Art. 1(4) of the Supplementary Agreement.
[158] Point 3.46 of the EDPS Authorisation Decision of 31 August 2021.

3.97. **However, despite these contractually binding obligations, the EDPS notes that it is unclear whether the Court has created a Single Point of Contact (SPoC).**[159] As assessed in Section 3.1.11. - **Condition 12**, he Court indicated that it limited the TAC Support Information to *'the persons designated to open a possible support case with Cisco'*. However, the Court has not clarified if these designated persons act through the SPoC, with the use of a functional mailbox or another way that precludes their identification or singling out, or rather in their own name with the use of their own credentials (name, email address and phone number). In addition, **the EDPS notes that the Court does not appear to anonymise nor pseudonymise the content of the Customer Case Attachment(s)**, nor manually provide the specific anonymised, or pseudonymised, data needed for the resolution of the problem.[160]

3.98. Hence, the EDPS considers that the Court **has partially complied with Condition 13. To fully comply with that condition the Court must still:**

(i) Confirm the creation of the Court's Single Point Of Contact with Cisco for technical assistance purposes, or provide the EDPS with clear information on the creation of the SPoC,

(ii) Take measures to ensure that the SPoC will provide Cisco with the anonymised or effectively pseudonymised data needed for the management of technical assistance requests, as also explained in Section 3.1.11 - **Condition 12**.

### 3.1.13. Condition 14: Training procedure in place

3.99. In the Authorisation Decision of 31 August 2021, the EDPS requested that the new contractual clauses must ensure that specific training procedures for personnel in charge of managing requests for access to personal data from public authorities will be developed, including on 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.[161]

3.100. The Court informed the EDPS that specific clauses were added in the Supplementary Agreement to address this Condition.

---

[159] The Court has not demonstrated that such a SPoC has been established since there is no mention thereof except in the analysed contractual provision.
[160] Whereas in the context of the EDPS Authorisation Decision of 31 August 2021, the Court pledged that it would 'examine whether the data submitted for the resolution of the incident can be anonymised or be replaced with a pseudonym', see point 3.66 of the afore-mentioned Decision.
[161] Condition 14 of the EDPS Authorisation Decision of 31 August 2021.

3.101. Article 1(4) of the Supplementary Agreement deleted Article 11(2) of the contract and added the new clause (Art. 11(2)(e)), which is also inserted in Exhibit A of the contract ( contractual clauses), Annexes 1a and 1b, Sections C, Point 3.

3.102. The clause added to contractual clauses reads[162]: '[t]*he 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.'*

3.103. In the first place, the EDPS notes that the inclusion of this new clause in the Supplementary Agreement and its Exhibits creates a contractual obligation and is legally binding commitment for the parties.[163]

3.104. In the second place, the EDPS considers that the new clause is fully in line with the requirements of Condition 14 as it confirms that Cisco has already put in place the required training procedures for personnel in charge of managing requests for access to personal data from public authorities.

3.105. Hence, the EDPS considers that the Court has **complied with Condition 14**.

[162] A clause of the same wording, but different formatting is added in Art. 1(4) of the Supplementary Agreement.
[163] Point 3.46 of the Authorisation Decision of 31 August 2021.

# 4. CONCLUSION

## 4.1. Temporary authorisation valid until 31 October 2024

4.1.1. The EDPS considers that:

- communication (video- /web-conferencing) tools are essential means for an EUI to continue performing its tasks and duties carried out in public interest, as well as for the management and functioning of the EUI;

- the Court of Justice carries out an essential function in the EU as the judicial authority of the European Union, in maintaining the rule of law and respect of the fundamental rights and freedoms of individuals and, in cooperation with the courts and tribunals of the Member States, in ensuring the uniform application and interpretation of EU law;

- the Court and Cisco demonstrated their commitment and intention to comply with the requirements of the Regulation by having advanced the implementation of the Conditions imposed in the EDPS Authorisation Decision of 31 August 2021[164];

- to achieve the full level of compliance required under the Conditions imposed in the EDPS Authorisation Decision of 31 August 2021, a certain period of time may be still needed, as it requires changes to the architecture and design of provided services and the related processing of personal data;

- it is reasonable and proportionate to authorise temporarily and conditionally the use of contractual clauses in this specific case, despite the continued shortcomings identified above.

4.1.2. Therefore, pursuant to Article 58(3)(e) of the Regulation, the EDPS authorises until **31 October 2024** the use of the contractual clauses between the Court of Justice of the EU and Cisco Systems Inc. US, submitted by the Court on 1 September 2022, as a means for adducing appropriate safeguards under Article 48(3)(a) of the Regulation in the context of transfers of personal data in the Court's use of Cisco Webex and related services.

4.1.3. The EDPS underlines that this Decision **is without prejudice to EDPS' investigative powers**, in particular under Article 58(1)(b) of the Regulation.

## 4.2. Conditions for the renewal of the authorisation

4.2.1. In order for the Court to ensure appropriate safeguards and an essentially equivalent level of protection with regard to international transfers of personal data to Cisco

[164] The EDPS also notes that Cisco demonstrates a general commitment to improve its practices, i.e. by adhering to the EU Cloud Code of Conduct.

or its sub-processors, including by remote access, the EDPS set the following **conditions** that the Court must meet **for the renewal of the authorisation**:

(i) Provide detailed information about the scope and application of the Webex Data Residency programme, in particular by identifying the effect of deployment of this programme, the personal data covered by it as well as the applicable level of data residency per type of personal data,

(ii) Clarify the notion of User Generated Data, in particular to explicitly include 'real time meeting data' in the category of User Generated Data, hence confirming that this data is covered by the Webex Data Residency,

(iii) Demonstrate if, how and to what extent covering personal data under the Webex Data Residency programme prevents remote access (by sub-processors and third countries' authorities) to data stored and/or processed in the EU,

(iv) Clarify if and to what extent transfers of personal data take place because of the Court's use of Cisco's Meeting Server, Private Meetings and Video Mesh,

(v) Further adapt the contractual clauses as follows:
- Clause 8(2) (Purpose limitation) and Clause 8(8). (onward transfers): must reflect that transfers can take place 'solely to allow tasks within the competence of the Court to be carried out under EU law';
- Clause 8(8) (onward transfers) must refer to compliance with the principle of data minimization;
- Clause 9(a) (Use of sub-processors) must delete '*(if so)*';
- Clause 14 (Local laws and practices affecting compliance with the Clauses) must only refer to restrictions under Article 25 of the Regulation and they may only be imposed by the Court;
- Clause 15 (Obligations of the data importer in case of access by public authorities) - see condition 9 on disclosure requests;
- Clause 16 (Non-compliance with the Clauses and termination) must provide that not only the data importer but also its sub-processors should promptly notify the data exporter if they are unable to comply with the clauses;
- Clarify that Exhibits B and C also form an integral part of the contractual clauses,

(vi) Assess to what extent the Privileges and Immunities of the Court based on Article 2 of Protocol VII of the Treaty on the Functioning of the European Union are recognized in the legal framework of Cisco Systems Inc. US or of its sub-processors,

(vii) Revise the list of sub-processors and remove those that are not actually involved in the processing,

(viii) Specify that any sub-processor should be subject to a contract including the appropriate SDPCs adopted by the Commission as well as to appropriate

supplementary measures included in the SDPCs to be tailored depending on the role of the sub-processor in the processing activity,

(ix) Include an obligation for Cisco (including its sub-processors) to notify any disclosure requests it receives to the Court at default and as a self-standing obligation,

(x) Include an obligation for Cisco (including its sub-processors) to redirect any disclosure requests to the Court and seek instruction from the Court at default and as a self-standing obligation,

(xi) Include an obligation for Cisco (including its sub-processors) to introduce a legal challenge against any access request at default and as a self-standing obligation,

(xii) Ensure that the obligations of Cisco International Limited UK correspond to those of Cisco Systems Inc. US under the contractual clauses,

(xiii) Ensure that Cisco certifies 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,

(xiv) Continue seeking that state of the art end-to-end encryption technology in line with the technical requirements of the use cases 1 and 3 of Annex 2 to the EDPB recommendations is adopted for all the Webex videoconferencing communications, without exceptions, unless the Court does not plan to use those devices that are not compatible with such technical requirements in any of its communications, independently from the level of risk for data subjects involved. Where the Zero Trust End-to-End Encryption is used, it has to be deployed for all usages, without a risk based approach,

(xv) Provide the EDPS with more detail on the organisational measures aimed at preventing that devices that are not compatible with said technical requirements are used, including on monitoring and enforcing procedures to ensure the effective use of the planned organisational measures,

(xvi) Confirm the creation of the Court's Single Point Of Contact with Cisco for technical assistance purposes, or provide the EDPS with clear information on the creation of the SPoC, and

(xvii) Take measures to ensure that the SPoC will provide Cisco with the anonymised or effectively pseudonymised data needed for the management of technical assistance requests.

4.2.2. The Court is required to ensure an essentially equivalent level of protection within **16 months**, i.e. 1 March 2024, by **remedying the compliance issues** identified in the present authorisation.

4.2.3. The Court is to provide the EDPS **an intermediate compliance report 12 months after the date of entry into force of this Decision**, i.e., 1 November 2023, demonstrating steps taken to implement the conditions set in this Decision, as well as **a final compliance report** at the expiry of the deadline identified in point 4.2.2. of this Decision.

4.2.4. This Decision shall take effect on 1 November 2022.

# 5. JUDICIAL REMEDY

5.1. Pursuant to Article 64 of the Regulation, any action against a decision of the EDPS shall be brought before the Court of Justice of the European Union within two months from the adoption of the present Decision and according to the conditions laid down in Article 263 TFEU.

Done at Brussels, 28 October 2022

Wojciech Rafał WIEWIÓROWSKI