EUROPEAN DATA PROTECTION SUPERVISOR

EDPS Decision authorising temporarily the use of *ad hoc* contractual clauses between the Court of Justice of the EU and Cisco for transfers of personal data in the Court's use of Cisco Webex and related services

31 August 2021

(Case 2021-0255)

Summary:

This Decision addresses the request from the Court of Justice of the EU for authorisation of contractual clauses pursuant to Article 48(3)(a) of (EU) 2018/1725 (the 'Regulation')[1]. Pursuant to Article 58(3)(e) of the Regulation, the EDPS authorises until 30 September 2022 the use of *ad hoc* contractual clauses between the Court of Justice of the EU, Cisco International Limited UK and Cisco Systems Inc. in the context of transfers of personal data in the Court's use of Cisco Webex and related services, given the special circumstances of the COVID-19 pandemic. The Court is to remedy the compliance issues identified in the present authorisation to ensure an essentially equivalent level of protection within one year from the date of this Decision, following which the EDPS will reassess the transfer authorisation and may order the suspension of data flows. The Court is to provide the EDPS an intermediate compliance progress report six months after the date of this Decision demonstrating the implementation of the conditions set for the renewal of the authorisation.

[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 authorisation of *ad hoc* contractual clauses (to be) concluded between the Court of Justice of the EU ("the Court"), Cisco International Limited UK 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. The Court submitted its request for authorisation on 23 February 2021, which due to transmission issues of a technical nature was received by the EDPS on 4 March 2021.

1.3. The Court attached a full copy of the contract and its annexes (Annex 1 to the Court's request letter), as well as the Data protection impact assessment (DPIA) and its annexes (Annex 2 to the Court's request letter) to its request for authorisation. According to the request for authorisation and the contract[2], in particular, the following **contractual clauses in the contract and its annexes are intended to provide appropriate safeguards in line with Article 48(3) of Regulation (EU) 2018/1725**[3] ('the Regulation') for transfers to third countries in the Court's use of Cisco Webex and related services:

- clause 11.2 (Processing of Personal Data by the Supplier) of the contract;
- Annex 1.d to the contract - Attachment A - Information Security Exhibit, and Attachment B –Contractual clauses providing appropriate safeguards for the transfer of personal data to third countries;
- Annex 1.f to the contract - Data Privacy Sheets: Attachment 1 - Webex Meetings Data Privacy Sheet, and Attachment 2 – TAC Data Privacy Sheet.

Based on the information provided by the Court in its request for authorisation and in its exchanges with the EDPS and with Cisco, the following contractual clauses in the contract are also intended to provide guarantees and safeguards for transfers "*to offer an equivalent level of protection of personal data*":

- clause 7.5 (Suspensive condition) of the contract,
- clause 14 (Security) of the contract,
- clause 19 (Termination) and
- clause 20 (Liability) of the contract.

[2] See clause 7.5 (Suspensive condition) of the contract.

[3] 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.

1.4. The Court also provided further information and clarifications on the circumstances of the processing and transfers of personal data, as well as on the commitments and measures taken or planned by the Court and / or by Cisco on 15 April 2021, 18 June 2021 and 5 and 15 July 2021.

1.5. It follows from these more recent information and clarifications that the contractual clauses that had been submitted to the EDPS for authorisation are outdated and will be heavily modified as the 2010/87/EU SCCs for transfers to processors under Directive 95/46/EC have been repealed with effect from 27 September 2021 and the Court intends to rely on the new standard contractual clauses adopted by the Commission on 4 June 2021[4] for transfers under the GDPR[5] ("new SCCs for transfers under the GDPR") as a *model* for their future *ad hoc* contractual clauses, which will also include updated commitments in the relevant clauses in the main body of the contract.[6]

1.6. The legal analysis and conclusions of the EDPS (sections 3 and 4 of this Decision) therefore in particular focus on the **safeguards and measures,** including **supplementary measures**, **that must be** provided **in the new *ad hoc* contractual clauses** to meet the EU standard of essential equivalence of protection.

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

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

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

[4] 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, OJ L 199, 7.6.2021, p. 31.

[5] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016, p. 1.

[6] See in this respect below sections 2 and 3 of this Decision.

(TAC) Service Delivery).[7] In order to offer an essentially equivalent level of protection of personal data when it is transferred outside the EU/EEA, the Court foresees a number of measures and clauses.

2.2. The contract has already entered into force for the other services (e.g. on-premise software Cisco Meeting Server, Cisco Unified Communications Manager), which are already in use by the Court. These on-premise services might also involve transfers of personal data to Cisco or its sub-processors, e.g. if support services were requested from Cisco in relation to an on-premise software[8], where an on-premise software would be transmitting telemetry data to Cisco or where a software like Cisco Video Mesh functions as a hybrid service allowing for on-premise and cloud-based use[9]. The contract however does not clearly provide appropriate safeguards for such transfers. It seems from the DPIA report that the Court is taking some technical and organisational measures to limit and/or prevent those transfers. However, as the contract and its annexes are generic and not specific to how the Court is implementing the software and services provided by Cisco, these measures do not seem to be included in the contract and its annexes and made binding.

2.3. For the use of Cisco cloud services requiring a transfer of personal data, the contract only enters into force upon the authorisation of the transfer and the necessary contractual clauses by the EDPS.[10]

2.4. The contract lists 32-35 types of personal data from four categories of data (registration(=user) information[11], host and usage information[12], user-generated information[13] and technical support assistance information) that may be concerned by transfers in the Court's use of Cisco Webex Meeting services. The contract lists 27 types of personal data from two categories of data (technical support assistance information and customer case attachment) that may be concerned by transfers in the Court's use of Cisco Technical Assistance (TAC) Service Delivery services.

---

7 According to the DPIA by the Court (p. 4), the Court will not use other services available under the product suites covered by the contract with Cisco. The Court purchases subscription to Cisco Collaboration Flex Plan Meetings Enterprise Agreements Suite, Cisco Collaboration Flex Plan Calling Enterprise Agreements Suite, as well as support services for cloud services and on-premise software. The services of the Meetings Suite can each be configured/deployed as either a cloud service or on-premise software. The services of the Calling Suite can be configured/deployed as either a cloud service, on-premise software or partner-hosted software. See clauses 3 and 4 at p. 4 of the contract and Annexes 1a and 1d to the contract.

8 See Cisco Unified Communications Manager Privacy Data Sheet available on the Cisco Trust Center Portal.

9 See the DPIA by the Court, p. 3.

10 See clause 7.5 (Suspensive condition) at p. 9 of the contract.

11 Name, Email, Address, Password, IP Address, Browser, Phone Number (Optional), Mailing Address (Optional), Geographic region, Avatar (Optional), User information included in the Your Directory (if synched), Unique User ID (UUID).

12 IP address, user agent identifier, hardware type, operation system type and version, client MAC address, meeting session information, call attendee information (including email address, IP address, username, phone number), performance, troubleshooting and diagnostics information etc.

13 Meeting and call recordings, polling data, transcriptions of call recordings, uploaded files. I.e. content data of a meeting.

2.5. The contract however sets out that personal data will only be processed within the European Union (EU) and the European Economic Area (EEA) and not leave the territory or be given access from outside the EU and the EEA. Personal data will be held in Webex data centres (both Cisco-owned and third-party provider - Amazon Web Services (AWS)) in The Netherlands and/or in Germany, which cannot be changed without prior written notification to the Court.[14] However, this seems to apply only to User Generated Information in use of Cisco Webex Meetings. Other types of personal data collected and processed in the use of Cisco Webex services or processed for other purposes, and personal data collected and processed in the use of Cisco Technical Assistance (TAC) Service Delivery services, as well as the processing of data stemming from use of Webex app do not seem to be covered by these transfers restrictions.[15] Transfers and onward transfers[16] of those not-covered types of personal data are therefore possible.

2.6. The contract sets out a temporary derogation from the above data localisation and access obligation in EU/EEA for transfers to the United Kingdom (UK) during the specified period laid down in Article FINPROV.10A (the "bridging clause") of the EU-UK Trade and Cooperation Agreement. At the end of the period under the "bridging clause" of the EU-UK TCA, the transfers will be covered either by an adequacy decision for the UK or appropriate safeguards under Article 48 EUDPR.[17] It is not clear which data would be transferred to which entities in the UK. This would seem to be User Generated Information in use of Cisco Webex Meetings transferred to Cisco or AWS data centre in London, UK.[18]

2.7. Cisco has agreed to take the necessary measures to end the transfer to the United States of America (US) of personal data that Cisco qualifies as Billing and Analytics Data in Attachment 1 to Annex 1f to the contract. Until then there is a temporary derogation until 31 December 2021 for the transfers to the US of that data, which can be extended by mutual agreement, and if Cisco cannot put an end to these transfers, the Court can also terminate the contract.[19] It is not clear to which categories and types of data, which may be concerned by transfers in use of various Cisco services, this qualification as Billing and Analytics Data corresponds to. Seemingly, Analytics Data corresponds to different types of data under Host and Usage Information stemming from use of Cisco Webex Meetings, which are collected and processed for various purposes, including analytics, service

---

[14] See clause 11.2(b)(i-iv) at p. 14 of the contract.

[15] See Annex 1d Attachment B - Appendix 1 and Annex 1f Attachments 1 and 2. See also DPIA by the Court.

[16] In line with recital 63 and Article 46 of the Regulation, an onward transfer is a transfer of personal data from a recipient in the third country of destination or a recipient in international organisation:
- to another third country or to another international organisation, or
- to another controller, processor or other recipient in the same third country or in the same international organisation.

[17] See clause 11.2(b)(v) at pp. 14-15 of the contract.

[18] See Annex 1f Attachment 1- Webex Meetings Data Privacy Sheet. See also DPIA report by the Court.

[19] See clause 11.2(b)(vi-vii) at p. 15 and clause 19 at p. 22 of the contract.

improvement and diagnosing technical issues.[20] Whereas Billing Data could correspond to different types of data under User Information stemming from use of Cisco Webex Meetings, which are also collected and processed for various purposes, including billing, service improvement and providing support.[21]

2.8. Neither does Annex 1d Attachment B to the contract clearly set out which of the data listed therein is transferred to which entity in which country for which purposes. Some information on cross-border transfers that might happen in context of Cisco Webex Meetings services[22] and Cisco Technical Assistance (TAC) Service Delivery services[23] is provided in Annex 1f to the contract, however the information on the location of data centres and sub-processors therein is subject to change by Cisco[24]. The contract provides that changes in respect to international transfers and the engagement of new sub-processors will be in all cases notified to the Court as soon as practically possible for Cisco and in no later than one month prior the change.[25]

2.9. The information on transfers of personal data in the contract and the contractual clauses and measures intended to provide appropriate safeguards initially submitted to the EDPS: i) do not include all the details on transfers, ii) have been changed since the signature of the contract or iii) are intended to be changed by the Court and Cisco.

2.10. From the information provided by the Court in exchanges with Cisco, the EDPS understands that in a first stage only billing and analytics data will no longer be transferred to the US, and in a second stage operational data (i.e. for ensuring security) will no longer be transferred. The EDPS also understands that after the conclusion of the EU Data Residency Program, ending transfers to the US, all personal data related to the use of Cisco Webex services will be stored/reside in the EU by Cisco International Limited UK or Cisco Systems International BV (NL).[26]

---

[20] See Annex 1f Attachment 1- Webex Meetings Data Privacy Sheet. See also DPIA report by the Court.

[21] See Annex 1f Attachment 1- Webex Meetings Data Privacy Sheet. See also DPIA report by the Court.

[22] It seems that cross-border transfers in context of Cisco Webex Meetings services might happen to Cisco establishments and its sub-processor Amazon Web Services to different third countries (US, UK, India, Singapore, Australia, Japan, Canada) - see Annex 1f Attachment 1- Webex Meetings Data Privacy Sheet, see also DPIA report by the Court. It seems from the description of Cisco services in the DPIA report that the Court would not be using Cisco services that would entail use of other two possible sub-processors Akamai and WalkMe, which may locate data globally.

[23] It seems that cross-border transfers in context of Cisco Technical Assistance (TAC) Service Delivery services might happen to Cisco establishments and its sub-processors (Amazon Web Services, Salesforce, Aricent, Estarta, Sykes, Concentrix) to different third countries (US, India, Jordan, Costa Rica, Columbia). See Annex 1f Attachment 2 – TAC Data Privacy Sheet.

[24] Cisco makes the most current Data Privacy Sheets for its different services available on the Cisco Trust Center Portal. The most current Webex Meetings Data Privacy Sheet available is Version 4.7, June 2021, whereas the on in Annex 1f to the contract is Version 4.5, January 2021.

[25] See clause 11.2 at p. 16 of the contract.

[26] According to Court exchanges with Cisco provided to the EDPS this is to include user information, host and usage information, user generated information, billing data and analytics data in the use of Webex, Webex with End-to-end Encryption and Webex with video Mesh and private meetings (with internal users

Furthermore, third-party sub-processors (e.g. AWS) already listed in the contract and pre-approved will remain the same as per the list provided in the Data Privacy Sheets[27] incorporated in the contract. Furthermore, while there will still be worldwide data transfers (including remote access) in provision of Cisco support (TAC) services, the EDPS understands that such support would in the first place be provided in and from Europe given that the customer is in the EU, before support would be provided from third countries (as part of the "Follow-The-Sun" workflow). The Court further clarified that as regards support in the use of Cisco Webex services the Court intends to rely primarily on support provided by the Court's internal and external services prior to relying on Cisco support (TAC) services.

2.11. Annex 1d to the contract contains in Attachment B specific contractual clauses providing appropriate safeguards for the transfer of personal data based on the 2010/87/EU SCCs for transfers to processors under Directive 95/46/EC.[28] According to the Court, they were adapted in order to take into account the Regulation, the specific situation of the Court as EU institution and the contractual relationship with Cisco. However, no significant change of those clauses compared to the 2010/87/EU SCCs for transfers under Directive 95/46/EC is apparent. They were complemented by a few additional provisions mainly in the main body of the contract in relation to pseudonymisation and encryption and notification, information and transparency by Cisco to the Court on disclosure requests received by Cisco. The EDPS will analyse these additional provisions in more detail in section 3 of this Decision, however they are providing for a seemingly limited protection.

2.12. On the basis of the contract as agreed by the Court and Cisco, and in the future on the new *ad hoc* contractual clauses to be concluded, the Court, Cisco International Limited UK and Cisco Systems Inc. plan to exchange the types of personal data mentioned above, in particular under paragraphs 2.3 and 2.5, to the United States, India, Mexico, Jordan, Costa Rica, Columbia, and other third countries where Cisco Group entities, Cisco affiliated companies and other sub-contractors (e.g. AWS, Salesforce) may be located. Transfers will also occur to the United Kingdom, Canada and Japan, which have been recognised by the European Commission as ensuring an adequate level of protection.

---

only) services. This data is to reside on EU data centres in Amsterdam and Frankfurt. According to Cisco's response "Frankfurt falls within the territory of Cisco International Limited (in UK), as per the Cisco's corporate structure (should it be Amsterdam, it falls within the territory of Cisco Systems International BV, in the Netherlands)". Furthermore, Cisco has started migrating Webex meeting sites for EU customers from the London data centre to the Frankfurt data centre, which Cisco will also propose to the Court.

[27] According to Court exchanges with Cisco provided to the EDPS, see in this respect Annex 1f Attachment 1 - Webex Meetings Data Privacy Sheet and Attachment 2 - TAC Data Privacy Sheet.

[28] Commission Decision 2010/87/EU of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council, OJ L 39, 12.2.2010, p. 5.

3. LEGAL ANALYSIS

3.1. EU standards of protection for transfers of personal data outside the EEA

3.1. Transfers of personal data to recipients outside the European Union ('the Union') may generate additional risks for data subjects, as the applicable data protection rules in the recipient's jurisdiction may be less protective than inside the Union. For this reason, the Union legislator adopted specific rules for such transfers in Chapter V of the Regulation (Articles 46 to 51 of the Regulation). In line with Article 46 of the Regulation, all transfers are subject to the other provisions of the Regulation and no provisions in Chapter V may be applied in order to ensure that the level of protection of natural persons guaranteed by the Regulation is undermined.

3.2. In line with Article 47(1) of the Regulation, personal data may be transferred to a third country or an international organisation where the Commission has decided pursuant to Article 45 GDPR or Article 36 LED[29] that the third country or an international organisation provides a standard with regard to data protection that is essentially equivalent to that within the EU, and the personal data may be transferred solely to allow tasks within the competence of the EUI to be carried out. The Commission has adopted adequacy decisions for transfers to the UK[30], Japan[31] and Canada[32]. However, no Commission adequacy decision exists concerning transfers to e.g. the US, India and Mexico.

3.3. In the absence of an adequacy decision, controllers and processors may transfer personal data to a third country[33] only if appropriate safeguards are provided, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available.[34] Standard data protection clauses adopted by the European Commission or by the EDPS and approved by the European Commission may provide for such appropriate safeguards.[35] Such safeguards may also be provided, subject to the authorisation from the EDPS, by contractual clauses

[29] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ L 119, 4.5.2016, p. 89 (also called "the Law Enforcement Directive" - LED).

[30] Commission Implementing Decision of 28.6.2021 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by the United Kingdom, not yet published in the OJ.

[31] Commission Implementing Decision (EU) 2019/419 of 23 January 2019 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by Japan under the Act on the Protection of Personal Information, OJ L 76, 19.3.2019, p. 1.

[32] Commission Decision 2002/2/EC of 20 December 2001 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided by the Canadian Personal Information Protection and Electronic Documents Act, OJ L 2, 4.1.2002, p. 13.

[33] Remote access by an entity from a third country to data located in the EEA is also considered a transfer.

[34] Article 48(1) of the Regulation.

[35] Article 48(2)(b) and (c) of the Regulation.

between the controller or processor and the controller, processor or the recipient of the personal data in the third country or international organisation ("*ad hoc* contractual clauses").[36] Where the processor is not an EUI, such safeguards may also be provided by binding corporate rules ("BCRs"), codes of conduct or certification mechanisms pursuant to points (b), (e) and (f) of Article 46(2) of GDPR.[37]

3.4. The transfer tool relied on must ensure that data subjects, whose personal data are transferred to a third country pursuant to that transfer tool, are afforded a level of protection in that third country that is essentially equivalent to that guaranteed within the EU by EU data protection law, read in the light of the Charter.[38] Standard contractual clauses for transfers (under Article 46 GDPR or Article 48 of the Regulation) mainly contain appropriate safeguards of a contractual nature[39] that may be applied to transfers to all third countries. In accordance with the interpretation provided in the Court's *Schrems II* judgment[40], where the transfer by the EUI or on its behalf relies on Article 48 of the Regulation or Article 46 GDPR transfer tools, supplementary measures may be necessary depending on the third country law/practices to ensure an essentially equivalent level of protection.

3.5. EUIs must therefore carry out an individual case-by-case assessment in accordance with the *Schrems II* judgment, to determine whether, in the context of the specific transfer, the third country of destination affords an essentially equivalent level of protection to that in the EU. The EUI, where appropriate in collaboration with the data importer in the third country, must carry out this assessment of the effectiveness of the proposed safeguards before any transfer (including by way of remote access) is made or a suspended transfer is resumed. The use of SCCs or another transfer tool (e.g. *ad hoc* contractual clauses, BCRs) does not substitute this individual case-by-case assessment in accordance with the *Schrems II* judgment.

3.6. The assessment by the EUI should take into consideration the specific circumstances of the transfer (e.g. categories of transferred data, purposes for which they are transferred and processed in the third country and how) and all the actors participating in the transfer (e.g. controllers, processors and sub-processors processing data in the third country), as identified in the mapping of the transfers. The EUI will also need to factor into this assessment any envisaged onward transfer.[41]

---

36 Article 48(3)(a) of the Regulation.

37 Article 48(2)(d) of the Regulation.

38 See paragraphs 96 and 103 of the Schrems II judgment and recitals 65 and 70 and Article 46 of the Regulation.

39 See paragraph 23 of the EDPB Recommendations 01/2020. The same is valid also for the other Article 46 GDPR / Article 48 of the Regulation transfer tools, (e.g. BCRs, codes of conduct or ad hoc contractual clauses).

40 Judgment of the Court of Justice of 16 July 2020 in case C-311/18, Data Protection Commissioner v. Facebook Ireland LTD and Maximillian Schrems ("Schrems II"), ECLI:EU:C:2020:559.

41 See Article 46 of the Regulation and paragraphs 33 and 34 of the EDPB Recommendations 01/2020.

3.7. Where the required essentially equivalent level of protection for the transferred data is not effectively ensured, because the law or practice of the third country impinges on the effectiveness of the appropriate safeguards contained in the used SCCs for transfers or another transfer tool, the EUI must implement contractual, technical and organisational measures to effectively supplement the safeguards in the transfer tool, where necessary together with the data importer.[42]

3.8. This process of assessing the level of protection in the third country and whether supplementary measures are needed, and then identifying effective supplementary measures, is commonly called a 'transfer impact assessment'. The methodology to be used is available in the EDPB Recommendations 01/2020[43] and, as regards the assessment of access by public authorities for surveillance purposes, in the EDPB Recommendations 02/2020 on European Essential Guarantees[44].

3.2. Assessment of the safeguards (to be) provided

3.9. Based on the above-mentioned EU standards of protection for transfers, *ad hoc* contractual clauses should include a series of guarantees, safeguards and commitments by the EUI and the recipient in the third country of destination to take actions and measures. The EDPS is of the opinion that new *ad hoc* contractual clauses, based on the model of the new SCCs for transfers under the GDPR adopted by the Commission in 2021 and including updated relevant clauses in the main body of the contract, could provide sufficient guarantees for transfers of personal data in the Court's use of Cisco Webex and related services, provided they are complemented with additional guarantees and supplementary measures to ensure that the processing will meet the requirements of the Regulation and ensure an essentially equivalent level of protection to that guaranteed in the European Economic Area (EEA), as explained below.

3.2.1. Need to know and control data flows

3.10. The contract, in particular the Annexes 1.d and 1.f, do not provide clear information on what personal data is likely to be transferred to which recipients (processors and sub-processors) in which third countries covered in the contract. In addition, the contract suggests that Cisco International Limited UK and Cisco Systems Inc. and other Cisco establishments and its affiliates are not the only (sub-)processors potentially engaged through the Court's use of Cisco Webex and related services.

---

42 See paragraphs 54 and Annex 2 of the EDPB Recommendations 01/2020.

43 EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, version for public consultation adopted on 20 November 2020 and version after public consultation adopted on 18 June 2021.

44 EDPB Recommendations 02/2020 on the European Essential Guarantees for surveillance measures, adopted on 10 November 2020.

This is because Cisco Webex Meeting and support (TAC) services are also hosted on cloud infrastructure and storage services provided by AWS and Cisco support (TAC) services might also engage services of other sub-processors.[45] The EDPS therefore takes 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.

3.11. From the information provided by the Court in exchanges with Cisco, the EDPS understands that since the signature of the contract, Cisco is in the process of stopping certain transfers to the US (billing and analytics data in the first stage and operational data in a second stage). According to the information provided by the Court, the temporary derogation for transfers to the US of billing and analytics data can be extended as often as the parties agree to an extension. The Court will evaluate the necessity of an extension in the light of the efforts of Cisco to comply with its commitment to end such transfers, any further evolution on the discussions on a new adequacy decision for the US, any evolutions with regard to the safeguards and protection offered to personal data within the US, as well as the evaluation of the measures put in place by the contract, or added to it following a review, to protect personal data.

3.12. From the information provided by the Court in exchanges with Cisco, the EDPS also understands that Cisco is in the process of adapting the architecture and design of the cloud offering, reorganising where data of its EU clients will reside (under the so called EU Data Residency Program), which will impact data flows (including by remote access) within and outside the EU/EEA, their recipients and consequently what safeguards and measures would be appropriate and effective.[46] The EDPS stresses that after the conclusion of the EU Data Residency Program there should be **no ambiguity** whether certain personal data from a specific service is stored, transferred (including by remote access) or otherwise processed in a specific country.

3.13. Information on **all data, all the actors and all the third countries involved** for transfers in the Court's use of Cisco Webex and related services is the minimum essential information for a meaningful 'transfer impact assessment' in line with the *Schrems II* judgment and the EDPB Recommendations 01/2020[47]. The utmost importance of absolute clarity in this regard was also stressed by the EDPB and the EDPS concerning the new SCCs proposed by the EC.[48]

---

45 See also paragraph 2.4. of this Decision.

46 See also paragraph 2.6. of this Decision.

47 See in particular Step 1 'Know you transfers' of the roadmap in the EDPB Recommendations 01/2020. In line with existing obligations in Articles 4, 5, 6, 9, 26, 29, 30 and Chapter V of the Regulation, the EUIs need to know and control data flows within and outside the EU.

48 See paragraphs 127 to 132 and annex of the EDPB-EDPS Joint Opinion 2/2021 on the European Commission's Implementing Decision on standard contractual clauses for the transfer of personal data to third countries for the matters referred to in Article 46(2)(c) of Regulation (EU) 2016/679.

3.14. The Court is required therefore to **possess a detailed knowledge of 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.** This is necessary so that the Court is in a position to: i) make meaningful a TIA, including identifying effective safeguards and measures[49], ii) implement those safeguards and measures itself and by Cisco, iii) complete annexes of *ad hoc* contractual clauses with all due diligence and iv) be able to demonstrate that all assessments have been made and measures implemented and effectiveness of those measures.

3.15. The EDPS welcomes changes being made by Cisco to how it will provide its services and the associated data flows within and outside the EU, as well as the Court's intention not to endlessly extend the temporary derogation for transfers to the US of billing and analytics data. The EDPS encourages the Court i) to make this into a binding commitment / obligation for the parties with a set deadline and/or a set limited number of extensions and ii) to make the evaluations of whether extension is necessary as explained in paragraph 3.11 an internal obligation for the Court.

3.2.2. Contractual safeguards and supplementary measures

Contractual commitments in the contract and its annexes

3.16. The **clauses in the contract as agreed by the Court and Cisco** do not appear to provide sufficient guarantees to provide an essentially equivalent level of protection, for the reasons set out below. Moreover, many of the initial clauses, commitments and details on transfers are **unclear, outdated and changing**, in particular since the adoption of the new SCCs for transfers under the GDPR, the 2010/87/EU SCCs for transfers to processors under Directive 95/46/EC have been repealed with effect from 27 September 2021. Furthermore, the Court brought to the EDPS attention an exchange of letters with Cisco describing further details of transfers and planned changes of transfers and of transfer safeguards and commitments on technical and organisational measures.

3.17. The Court expressed its intention to rely on **new *ad hoc* contractual clauses**, based on the **new SCCs for transfers under the GDPR**, **including updated commitments in** the main body of **the contract**. At the beginning of 2021, Cisco also made commitments to its customers to "*update its MDPA [(Master Data Protection Agreement)] to include the new SCCs and rollout for EU based Customers, Partners, and Suppliers during the transition period.*"[50]

---

[49] Identification of effective safeguards and measures is part of the TIA (steps 2 and 4 in EDPB Recommendations 01/2020).

[50] See question 3 International Transfer of Personal Data post-Schrems II FAQ, available on the Cisco Trust Center Portal.

3.18. The EDPS and the EDPB have issued joint opinions on the draft SCCs between controllers and processors[51] and on the draft SCCs for the transfer of personal data to third countries under the GDPR[52], as proposed by the Commission. The Court may find those joint opinions useful when it will be adapting the new SCCs for transfers under the GDPR to the Regulation and including details on the transfers and additional safeguards and commitments.

Imposing clear and binding obligations on all recipients

3.19. The Court concluded the initial contract with Cisco International Limited UK and a number of its annexes with Cisco Systems Inc. US. However, it appears unclear how the provisions of the contract, in particular those relating to transfers[53], bind other Cisco establishments (e.g. Cisco 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 Inc. or its applicable affiliates. In particular, the Annex 1d Attachment B (signed by Cisco Inc.) sets out that any reference to "data importer" means Cisco, whereas in Annex 1d Attachment A reference to "Cisco" means the Party receiving Protected Data. It is not clear how the obligations and commitments in the Court's contractual clauses have been passed on to sub-processors within and outside Cisco Group.

3.20. According to the clarifications provided by Cisco to the Court, **Cisco's corporate data protection compliance policies** implemented by Cisco Systems, Inc. are binding and compulsory for all Cisco Group companies and all of Cisco's workforce. This includes its Global Personal Data Protection and Privacy Policy, as well as a Group Personal Data Transfer Agreement that *"obligates Cisco entities located outside the EU/EEA in a jurisdiction not providing adequate protection to process personal data in accordance with the terms of the Standard Contractual Clauses*".[54] The EDPS understands the Group Personal Data Transfer Agreement as being Cisco's pre-GDPR approved **Binding Corporate Rules** when Cisco processes personal data as a controller. Cisco is however processing personal data as processor in the Court's use of Cisco Webex Meeting and related services. In this respect, according to Cisco, Cisco submitted in September 2020 its application for approval of Binding Corporate Rules when Cisco acts as a data processor (e.g., when providing services on behalf of its customers), which will also serve as an additional legally valid

---

51 https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-12021-standard_en

52 https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-22021-standard_en

53 E.g. under clause 11.2(b) of the contract.

54 According to the clarifications provided by Cisco to the Court, "[a]ll Cisco affiliates are covered by the terms of the so called Intercompany Transfer Agreement (ITA) with respect to processing of personal data. Thus, these can be considered as sub-processors acting on behalf of the processor (the Cisco entity entering into an agreement) whose processing is based on the SCC's (the transfer mechanism that the company group relies on).".

transfer mechanism when approved.[55] The EDPS understands that **none** of these documents however **apply to other sub-processors not part of the Cisco Group**.

3.21. As recalled in paragraph 3.13 above, EUIs as controllers for the processing need to know and control data flows. This means that they must ensure that the contractual safeguards and supplementary measures impose clear and binding obligations on all envisaged recipients in third countries to which personal data will be transferred (including by remote access).

3.22. The Court therefore must conclude the new *ad hoc* 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). Adherence to the new *ad hoc* contractual clauses concluded by the Court 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.[56]

3.23. The Court is to ensure that the provisions of the new *ad hoc* contractual clauses, including those in the main body of the contract[57], apply to and are binding upon other Cisco establishments (e.g. Cisco Inc. US), its affiliates, partners and sub-processors and are not rendered ineffective by the concurrent application of other obligations Cisco may impose on them (e.g. intra-corporate agreements).

3.24. The new *ad hoc* clauses must therefore 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.

3.25. If the other recipients do not adhere to the new *ad hoc* 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.

---

55 See question 6 in International Transfer of Personal Data post-Schrems II FAQ, available on the Cisco Trust Center Portal.

56 See Section III, Clause 7 ("Docking clause") of the new SCCs for transfers under the GDPR.

57 In particular e.g. clause 11.2(b) of the contract.

Necessary and appropriate contractual supplementary measures

3.26. The EDPS notes that the contract and its annexes lists different third countries and different recipients to which personal data in the use of different Cisco Webex and related services may be transferred. The EDPS also notes that, according to Annex 1f to the contract, some services are organised globally, and that, for instance, personal data in the use of Cisco support (TAC) services may be transferred to any third country where Cisco or its sub-processors operate such services.

3.27. The new SCCs for transfers adopted by the Commission include that 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 prevent the data importer from fulfilling its obligations under the SCCs.[58] The EDPS stresses that the assessment of whether there is or not any such reason and then implementation of any necessary safeguards and measures to supplement[59] safeguards present in the SCCs are to be done *before* the SCCs are signed.

3.28. As recalled in paragraph 3.5 above, Article 46 GDPR or Article 48 of the Regulation transfer tools mainly contain appropriate safeguards of a contractual nature that may be applied to transfers to all third countries.[60]

3.29. These could be third countries where SCCs, may, together with safeguards and measures (e.g. those in accordance with Articles 33 and 36 of the Regulation) already foreseen by the controller and processor, ensure an essentially equivalent level of protection. Such may be the case for transfers to a country that has applied for accession to the EU (e.g. Serbia), which, while not benefitting from an adequacy decision of the Commission has, as a candidate country for accession to the EU, signed binding international commitments and is in the process of transposing EU legislation into its national legislation to harmonise it to that of the EU *acquis*[61]. Such may also be the case for transfers to a country for which the Commission is in the process of adopting an adequacy decision, like South Korea.

3.30. However, there are third countries (such as the US, India, Mexico, Jordan) to which personal data may be transferred through use of Cisco Webex and related services where the SCCs are unlikely alone to provide essentially equivalent protection. For example, according to Cisco, Cisco is subject to FISA 702 in the US for certain of

---

58 See Section III, Clause 14 ("Local laws and practices affecting compliance with the Clauses") of the new SCCs for transfers under the GDPR.

59 Any contractual supplementary measures and contractual commitments to implement technical and organisational measures that the EUIs identified during the transfer impact assessment.

60 See paragraph 23 of the EDPB Recommendations 01/2020.

61 E.g. a Stabilisation and Accession Agreement between the EU and the candidate country provides obligations of harmonisation of the country's national law with EU law, including fundamental rights and data protection law.

Cisco service offers.[62] Jordan is a third country without a data protection law and without a data protection authority.[63] Additional contractual, technical and organisational measures ("*supplementary measures*") to ensure the required level of protection will thus be required for such countries.[64] Some measures may be effective in one situation while not effective in another. The situation in different third countries to which personal data will be transferred may therefore require different approaches and different combinations of supplementary measures.

3.31. Annex 2 of the EDPB Recommendations 01/2020 gives examples of supplementary measures, as well as use cases and conditions for effectiveness of the measures. The Court should consider all examples therein, 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.

Privileges and immunities

3.32. The initial contractual clauses contain as a safeguard for transfers a provision recalling that the Court is subject to Protocol 7 of the Treaty on the Functioning of the European Union on the privileges and immunities of the EU, particularly as regards the inviolability of archives (including the physical location of data and services as set out in clause 11.2 of the contract) and data security, which includes personal data held on behalf of the Court in the premises of Cisco or subcontractor.[65].

3.33. The EDPS considers 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

---

62 According to Cisco, "Cisco is not directly subject to surveillance requirements under EO 12333 nor voluntarily cooperating with any program authorized by the EO. Most Cisco offers are also not subject to FISA 702. However, Webex Teams, Meetings, Meraki and other Cisco SaaS offers are considered electronic communication services or remote computing services. Therefore, customer data transferred and processed in connection with these select offers may, theoretically, be within the scope for a FISA 702 demand – if such data is related to foreign intelligence necessary for national security purposes. ...". See question 9 in International Transfer of Personal Data post-Schrems II FAQ, available on the Cisco Trust Center Portal.

63 https://privacyinternational.org/state-privacy/1004/state-privacy-jordan

64 See Step 4 'Adopt supplementary measures' of the roadmap in the EDPB Recommendations 01/2020. "Supplementary measures" are by definition supplementary to the safeguards the Article 48 of the Regulation - or Article 46 GDPR - transfer tool already provides and to any other applicable security requirements (e.g. technical security measures) established in the Regulation or the GDPR.

65 See clause 11 at p. 17 of the contract. See also clause 10.2 at p. 13, which in application of the principles of inviolability of premises and archives of the EUIs, established by the Protocol 7, prohibits compliance audits by Cisco of the Court 10.2 Customer's Compliance.

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[66]. This was contrary to Articles 4(1)(f) and 49 of the Regulation.

3.34. As part of the transfer impact assessment, the Court should verify to which extent

(i) the privileges and immunities, as extended to the Court by a third country of destination, apply to and are binding upon the public authorities in that third country and are not rendered ineffective by the concurrent application of other obligations of the third country's authorities[67];
(ii) the Court (as controller of the data transferred to and held by Cisco and its sub-processors on the Court's behalf) is in a position to effectively defend against disclosure requests[68] not authorised by EU law from third country governments, by relying on its privileges and immunities; and
(iii) Cisco and its sub-processors subject to third-country jurisdiction are able to notify and redirect disclosure requests they receive to the Court and legally challenge disclosure requests invoking privileges and immunities extended to the Court.

Commitments concerning disclosure requests from third country authorities

3.35. The initial contractual clauses contain as a safeguard for transfers a clause with transparency obligations and commitments from Cisco to take certain actions in case of disclosure requests from third countries. The contract provides that, unless prohibited by applicable law[69], Cisco shall **notify** the Court of **any legally binding request** for disclosure of the personal data processed on behalf of the Court 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, Cisco may not give such access without the prior written authorisation of the Court. Cisco shall challenge a prohibition to notify the Court by exhausting all legal remedies, including interim measures, and shall use all possible efforts to obtain the right to waive this prohibition in order to communicate as much information as they can and as soon as possible.[70] According to the contract, Cisco shall be able to demonstrate that it did so to the Court.

---

66 See pp. 45-49 of EDPS report of March 2020 on the investigation into the use of Microsoft products and services by Union institutions, bodies, offices and agencies (the 'the March 2020 Investigation Report'), section 7 'Unauthorised disclosure' and respective recommendations.

67 As defined by the relevant US legislation, e.g. 50 U.S.C. § 3003(4).

68 In actions or appeals against such disclosure requests as provided in the third country laws, applicable obligations under international law and principles of international comity.

69 Presumably, applicable law of the (third) country of the recipient is meant here and not the applicable law as set out in clause 22 of the contract (EU law complemented by the law of Luxembourg).

70 See clause 11.2 at pp. 17 and 18 of the contract.

3.36. Cisco will, furthermore, provide the Court at the end of each annual period an **Overview Statement of all disclosure requests received**. The Overview Statement must include a full list of all requests received (without exception) during the previous year or a statement that no requests have been received during the previous year, if this is indeed the case.[71]

3.37. The EDPS welcomes the inclusion of these additional provisions in the contract. However, following the Schrems II judgment all these commitments should be strengthened in line with the contractual supplementary measures of Annex 2 of the EDPB Recommendations 01/2020.[72]

3.38. These safeguards would only provide limited protection in case applicable law prohibits the notification and information[73]. This would entail, for instance, that Cisco will not notify the Court a request for disclosure if Cisco were prohibited to do so by the applicable law of a third country; Cisco is under no obligation to provide information (Overview Statement) if it were barred from providing disclosure of one or more such requests due to legal obligations. In light of prohibitions imposed by e.g. the US surveillance legislation, these clauses therefore only provide for limited protection.

3.39. The protection by these additional provisions in the contract would seem to be even more limited as their application to other Cisco establishments (than Cisco International Limited UK), Cisco affiliates and other sub-processors. Some commitment to **inform** the Court **if** Cisco is **prevented or unable to comply with the clauses and its commitments** due to legal obligations imposed by third country legislation is included in Annex 1d Attachment B as part of the 2010/87/EU SCCs for transfers to processors under Directive 95/46/EC.

3.40. Contractual measures will not be able to rule out the application of the legislation of a third country which does not meet the EDPB European Essential Guarantees standard in those cases in which the legislation obliges importers to comply with the orders to disclose data they receive from public authorities.[74]

3.41. As stressed by the EDPB, contractual obligations imposed on the data importer (recipient) concerning disclosure requests from third country authorities is a means to ensure that the data exporter (controller) becomes and remains aware of the risks attached to the transfer of data to a third country.[75]

---

71 See clause 11.2 at pp. 17 and 18 of the contract.

72 See paragraphs 105 to 121 of the EDPB Recommendations 01/2020.

73 Presumably, applicable law of the third country is meant here and not the applicable law as set out in clause 22 of the contract (EU law complemented by the law of Luxembourg).

74 See paragraph 101 of the EDPB Recommendations 01/2020 and paragraph 125 of the Schrems II judgment.

75 See paragraph 108 of the EDPB Recommendations 01/2020.

3.42. Such contractual obligations will enable the data exporter to desist from concluding a contract if the law of the third country, the safeguards contained in the transfer tool used and any additional safeguards supplementing the transfer tool cannot ensure a level of protection essentially equivalent to that in the EEA.[76]

3.43. Where the law and practice of the third country of the data importer was initially assessed and deemed to provide an essentially equivalent level of protection as provided in the EU for data transferred by the data exporter, and the information changes following its conclusion, such contractual obligations will enable the data exporter:

(i) to become aware of any changes in the situation in that third country following the conclusion of the contract, and
(ii) to reassess the situation and implement any additional supplementary measures to supplement the transfer tool used to effectively ensure a level of protection essentially equivalent to that in the EEA, or
(iii) to fulfil its obligation to suspend the transfer and/or terminate the contract if the law of the third country, the safeguards contained in the transfer tool used and any additional safeguards it may have adopted can no longer ensure the essentially equivalent level of protection.[77]

3.44. The new *ad hoc* contractual clauses must contain clear obligations and binding commitments from Cisco to notify and redirect to the Court any disclosure requests for Court's data that Cisco, its affiliates or its sub-processors receive and to legally challenge such disclosure requests.

'No backdoor policy and other principled approach provisions'

3.45. According to the exchanges between the Court and Cisco, Cisco indicated it is willing to add to the contract explicit language with regard to its "no backdoor policy". Cisco informed the Court that they are "prepared to work with the CURIA and formulate expressly a clear statement regarding the so called 'no backdoor policy' Cisco follows, as described in details in the Cisco Secure Development Lifecycle document[78]".

3.46. The EDPS notes that the Cisco Secure Development Lifecycle document from Cisco is a standard IT development process description, without any such assurance. In line with the EDPB Recommendations 01/2020 however, the '**no backdoor policy and other principled approach provisions**' are part of the contractual supplementary measures that may need to be included in transfer tools following

[76] Ibid.
[77] See paragraph 108 of the EDPB Recommendations 01/2020.
[78] https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-secure-development-lifecycle.pdf

the Schrems II judgment.[79] The EDPS strongly recommends including such additional clauses in the Court's contract that turn Cisco's principled approach[80] into a contractual obligation and legally binding commitment for the parties.

3.47. As the EDPB points out, 'no back door policy' clause is important to guarantee an adequate level of protection of the personal data transferred and should usually be required. The existence of legislation or government policies preventing importers from disclosing this information may render this clause ineffective. The importer will thus not be able to enter into the contract or will need to notify to the exporter of its inability to continue complying with its contractual commitments.[81]

3.48. The new *ad hoc* contractual clauses need to 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.

3.2.3. Technical supplementary measures

Encryption of the Webex video-communications (provided as cloud service)

3.49. WebEx Meetings and Teams includes an **end-to-end encryption** option **for** communications under which the **meeting content** (i.e., video, audio, text, and files) cannot be deciphered by Cisco. According to the DPIA, the Court is engaged to start testing end-to-end encryption by default (at the level of setting parameters of the tools) with private keys not in Cisco's possession for videoconferences set in the cloud (and in particular with external participants).[82]

3.50. The EDPS understands that end-to-end encryption meetings are possible in certain situations. However, at least in one of the following situations (not exhaustive list) *no* end-to-end encryption is possible: use of third-party video endpoints, use of Cisco Webex Meetings Web App, use of Linux clients, use of Video-devices, Public Switched Telephone Network (PSTN) Call-in/Call-back. This means that only if all participants use Windows Webex clients (and only those) an end-to-end encryption meeting can take place.

---

79 See paragraph 109 of the EDPB Recommendations 01/2020.
80 https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-principled-approach-to-government-requests-for-data.pdf
81 See paragraph 110 of the EDPB Recommendations 01/2020.
82 See DPIA report by CJEU at pp. 3, 4 and 8.

3.51. According to the information provided by Cisco to the Court, "[b]y August 2021, all then-shipped devices and current clients will support this level of encryption for customers.", which the EDPS understands as meaning the new end-to-end encryption technology named '**Zero Trust Security for Webex Meetings**'. According to Cisco's reply and information on Zero Trust Security page[83], Cisco's Zero Trust Security for Webex meetings has three layers: identity verification (with end-to-end encryption), secure key exchange (with Messaging Layer Security (MLS) protocol) and end-to-end encryption for content protection (with Secure Frames (SFrame) encryption framework for encrypting real-time media). The EDPS understands that the Court will examine the use of this new end-to-end encryption solution.

3.52. According to Cisco, neither the current encryption feature, nor the first iteration of Zero Trust Security for Webex is supported for all meetings.[84] The EDPS understands that Cisco's future development of this new technology will also support browsers[85], however not when joining by telephone. The EDPS notes that this type of meetings have certain limitations where the server cannot have access to the conversation that might be needed for e.g. some features to be provided.[86] This means that according to the business case, the Court can still initiate non end-to-end encrypted meetings with external participants, the personal data of whom are accessible by Cisco. However, according to the future directions on the Zero Trust Security page, Cisco will improve end-to-end encrypted meetings to offer "ubiquitous E2E security" for every Webex meeting.

3.53. According to the information on Cisco Zero trust Security for Webex page, the EDPS understands that:

(i) Cisco currently automatically and reliably manages the identity verification and the keys;
(ii) Cisco does not have access to the keys and cannot access the meeting due to the end-to-end verification of identity component;
(iii) the keys are automatically rotated and at the end of the meeting, any remaining participants' keys deleted, so that even if the content of the end-to-end encrypted meeting was stored somewhere, it can no longer be decrypted;

---

83 https://www.cisco.com/c/en/us/solutions/collateral/collaboration/white-paper-c11-744553.html

84 https://help.webex.com/en-us/5h5d8ab/End-to-End-Encryption-with-Identity-Verification-for-Webex-Meetings

85 https://www.cisco.com/c/en/us/solutions/collateral/collaboration/white-paper-c11-744553.html

86 Features provided by Cisco cloud services that require access to decrypted media, including:
- Recording to the cloud
- Transcoding media
- Webex Assistant for Webex Meetings (• Automated closed captioning, • Transcription)
- Saving session data, transcripts, meeting notes, etc. to the cloud (local recording and saving is supported)
- Public Switched Telephone Network (PSTN)
- SIP interoperability.

(iv) according to information about the future direction, in particular according to the future directions on the Zero Trust Security page, Cisco will improve end-to-end encrypted meetings to offer "decentralised identity" to allow customers to use their own end-to-end certificate authorities.

3.54. The EDPS recalls that US data importers that fall under FISA 702 are under a direct obligation to grant access to or turn over imported personal data that are in their possession, custody or control. This may extend to any cryptographic keys necessary to render the data intelligible. Hence, as stated in the EDPB Recommendations 01/2020, in situations where the keys are not retained solely under the control of the data exporter, or where the processing by cloud services providers or other processors require access to data in the clear, encryption does not provide for an effective supplementary measure necessary to bring the level of protection of the data transferred up to the EU standard of essential equivalence[87]. The same can be said when such encryption is already foreseen as a safeguard contained in the transfer tool relied on to transfer personal data.

3.55. In the EDPS' view, Cisco does not require access to the video-conferencing content data in the clear (i.e. not see the conference), in order to provide video-conferencing communication services. Encryption (transport encryption and end-to-end content encryption) could be considered an effective supplementary measure where a situation of use cases 1 and 3 of Annex 2 to the EDPB Recommendations 01/2020 applies. In line with the EDPB Recommendations 01/2020, the contract may need to provide that for transfers to take place, the data importer also commits to put in place the necessary technical measures identified by the data exporter.[88]

3.56. The EDPS notes that current end-to-end encryption solution is based on legacy technologies that do not support browsers and have serious limitations in the features of the service, and that only work with appropriate Cisco client software. The EDPS understands that the new end-to-end encryption solution will be based on different more open technologies that will make it possible to support also browsers and have more supported features. In addition to that, the new technology offers the assurance that (i) encryption keys are under the sole control of the intended participants, (ii) the identity of the participants can be verified, and (iii) it is not possible for a malicious entity to monitor the conversation without being noticed. The EDPS therefore considers that this new technology covers the requirements for use cases 1 and 3 of Annex 2 to the EDPB Recommendations 01/2020.

3.57. The new *ad hoc* 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[89] are adopted for *all* the Webex

[87] See paragraphs 81, 84, 94 and 95 of the EDPB Recommendations 01/2020.
[88] See paragraphs 103 and 104 of the EDPB Recommendations 01/2020.
[89] See in this regard paragraphs 90 and 94 of the EDPB Recommendations 01/2020.

videoconferencing communications, using state of the art end-to-end encryption technology.

Pseudonymisation of user information transferred to Cisco

3.58. According to the contract, certain user identifying information of the **Court's staff** members (name and email address) would be pseudonymised, by replacing it with an **internal pseudonym**, which would be transferred to Cisco. Since the Court informed the EDPS that it has decided not to implement this specific supplementary measure, the EDPS will therefore not comment on it.

3.59. According to the information provided by the Court, a **pseudonym** could, however, still be considered for certain events involving **external participants** and a generic account can also be used for such events by the host/organiser. the Court mentions "internal measures the Court can take in order to assure that external user are not obliged to provide this information", i.e. the user information that Webex requires when joining a meeting (mainly email address, phone number, name).

3.60. Additionally, the Court mentions another feature, which is not yet in full production: "In order to avoid the processing of "User generated information", the user can also activate the option "**Private meetings**". This option is currently available for testing (beta version) and it is attended that the definitive version will be available in July. The Court will adopt an internal measure to assure its use for internal meetings.". By using such feature, the personal data from the data category 'user generated information' would be replaced with **pseudonymous identifiers**. According to the information provided by the Court and Cisco, it seems that this measure is applicable to **internal users**.

3.61. In the EDPS' view, the proposed solutions do not cover all data categories and all user categories. In both solutions, extensive amount of other data allowing for identification / singling out of the data subject (staff and other participants/users) would still be sent to Cisco (e.g. IP addresses, numerous device identification data, data related to meetings and usage information).

3.62. Pseudonymisation could be considered an effective supplementary measure where a situation of use case 2 of Annex 2 to the EDPB Recommendations 01/2020 applies. In line with the EDPB Recommendations 01/2020, the contract may need to provide that for transfers to take place, the data importer also commits to put in place the necessary technical measures identified by the data exporter.[90]

3.63. The EDPS recalls that for pseudonymisation to be considered an effective mitigating measure and safeguard when personal data is transferred to a third country, a number of conditions described in the EDPB Recommendations 1/2020 should be

[90] See paragraphs 103 and 104 of the EDPB Recommendations 01/2020.

present, in particular as regards additional information, with the main aim of reducing the possibility of singling out data subjects, linkability and inferences[91]. Pseudonymisation is not an effective measure when the provider has additional information that allows re-identification or singling out of data subjects and is processing personal data in some cases in the clear.

3.64. The new *ad hoc* 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 (pseudonymization, access controls, special training module for administrators etc.) is adopted, so that Cisco effectively does not have access to personal data.

Access control in the use of Cisco support services (TAC) and Remote Access

3.65. According to the contract, Cisco has implemented organisational and technical **measures to control access by Cisco personnel** to customer data in the services.

3.66. The Court will also implement measures as follows:

"The Court has recourse to another service provider for first level support. Any request for support for the use of Cisco products will be handled internally within the Court and by the helpdesk service provider. Only in the event of problems that cannot be solved, the IT staff of Court (and not the end users) will have recourse to the TAC support of Cisco. In that event, the Court can also examine whether the data submitted for the resolution of the incident can be anonymized or be replaced with a pseudonym. Only in the event that this is not possible, personal data from a user will have to be transmitted to Cisco in the framework of TAC support."

3.67. According to the information Cisco provided to the Court, "The only possibility for remote access of personal data (constituting indeed transfer), as acquired via the provision of the Webex Meetings cloud-based offering of Cisco, is if and when Cisco technical assistance service ("TAC") may be requested to cover as support the functioning of the offering. ", and "should a customer located in Europe open a case for TAC support during the standard business hours in Europe, the TAC case will be picked up for support to be provided by the European TAC operations. If, however, due to technology expert availability or the priority level a TAC case may have been given by a customer, there's no or limited possibility for support to be provided by the European TAC operations then such TAC support will be provided outside of the EU/EEA (namely, APAC and US)."

[91] See paragraphs 85 to 89 of the EDPB Recommendations 01/2020. See also Article 29 Working Party. "Opinion 05/2014 on Anonymisation Techniques" (WP 216).

3.68. Transfers of personal data in the provision of these services would 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 would require access to data in the clear. In this respect, the EDPS recalls that where the processing by cloud services providers or other processors requires access to data in the clear and where the power granted to public authorities of the recipient country to access the transferred data in question goes beyond what is necessary and proportionate in a democratic society, the EDPB is, considering the current state of the art, incapable of envisioning an effective technical measure to prevent such access by public authorities from infringing on the data subject's fundamental rights.[92] Furthermore, access controls, access logs and other similar trails that do not or cannot[93] distinguish between accesses due to regular business operations and accesses due to orders or requests for access from third country public authorities do not constitute an effective measure.

3.69. Based on the information provided by the Court and Cisco, organisational measures proposed by the Court could be relied on to ensure that:

(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 anonymized data needed for the resolution of the problem, while Cisco will delete these data upon resolution of the problem;
(iii) apart from the data received by the Court SPoC, Cisco shall not have access to other Court data.

3.70. Corresponding contractual commitments to implement the organisational measures as identified under paragraph 3.63. above need to be included in the new *ad hoc* contractual clauses to be concluded by the Court, Cisco International Limited UK and Cisco Systems Inc.

3.2.4. Organisational supplementary measures

3.71. According to the Court, no further technical or organisational measures to ensure the essentially equivalent level of protection for the transferred personal data that could be used in the present circumstances have been identified.

3.72. The EDPS considers that implementing additional organisational measures may contribute to ensuring consistency in the protection of personal data in third countries.

---

[92] See paragraphs 94 and 96 of the EDPB Recommendations 01/2020.

[93] E.g. because the legislation of the third country (such as in the US) prohibits the data importer from informing the controller about the disclosure request received.

3.73. The new *ad hoc* 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.[94]

Transparency reports by Cisco

3.74. According to the contract[95] and the information provided, Cisco publishes a transparency report[96] containing general information about data access requests its receives[97].

3.75. The EDPS recalls that in order for a published transparency report to be effective, it should provide for information that is as relevant, clear and detailed as possible. When legislation in the third country prevents disclosure of detailed information, the data importer should employ its best efforts to publish statistical information or similar type of aggregated information[98].

3.76. Transparency reports can be a source of information to assess a third country on the condition that they expressly mention the fact that no access requests were received. Transparency reports merely silent on this point would not qualify as sufficient evidence as these reports most often focus on access requests received from law enforcement authorities and provide figures only on this aspect while remaining silent on access requests for national security purposes received. This does not mean that no access requests were received but rather that this information cannot be shared.[99]

94 See paragraph 131 of the EDPB Recommendations 01/2020.
95 See Section 9.f of Annex 1c - Universal Cloud Agreement to the contract.
96 https://www.cisco.com/c/en/us/about/trust-center/transparency.html
97 According to Cisco, "Cisco may receive demands from U.S. national security organisations. This includes FISA warrants, orders, directives or National Security Letters (NSLs).". See https://trustportal.cisco.com/c/r/ctp/trust-portal.html#/1625062361519106
98 See paragraphs 135 and 136 of the EDPB Recommendations 01/2020.
99 See paragraph 47 and Annex 3 of the EDPB Recommendations 01/2020.

4. CONCLUSION - TEMPORARY AUTHORISATION

4.1. Temporary authorisation valid until 30 September 2022

4.1. The EDPS considers that:

- in the context of the ongoing COVID-19 pandemic[100], 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; having a functional video-/web-conferencing tool during the crisis is thus of an imperative and vital importance;

- 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 stated their commitment and intention to comply with the requirements of the Regulation and to ensure the essentially equivalent level of protection of data subjects:

  - by having implemented a number of measures and clauses as data protection safeguards, as well as
  - by taking further actions in that respect and making changes as regards the processing, including associated data flows;

- to achieve that level of compliance, a certain period of time may be needed, as significant changes to

  - the architecture and design of provided services,
  - the related processing of personal data and
  - the respective data protection safeguards in order to comply with the Schrems II judgment

  are changes that are difficult to put in place immediately,

it is reasonable and proportionate to authorise temporarily the use of *ad hoc* contractual clauses in this specific case, despite the shortcomings identified above.

4.2. Therefore, pursuant to Article 58(3)(e) of the Regulation, the EDPS **authorises until 30 September 2022 the use of *ad hoc* contractual clauses** between the Court of Justice of the EU, Cisco International Limited UK and Cisco Systems Inc. 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.

[100] https://www.ecdc.europa.eu/en/covid-19

4.2. Conditions for the renewal of the authorisation

4.3. 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 or its sub-processors, including by remote access, the EDPS sets the following **conditions** that the Court and Cisco are to meet **for the renewal of the authorisation**:

1. The Court clearly identifies, in detail and without ambiguities, which personal data from which services will be transferred (including by remote access) for which purpose to which recipients in which third country with which safeguards and measures.

2. 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, will be stored/reside in the EU, in accordance with the contract concluded between the Court and Cisco[101]. In particular, Webex meeting and connection data (including personal data) in the Court's use of Cisco Webex services (whether on-premise 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.

3. 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[102], 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 SCCs 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.

4. The new *ad hoc* contractual clauses are concluded based on the model of the new SCCs for transfers under the GDPR adopted by the COM as adapted to the Regulation, include updated relevant clauses in the main body of the contract[103] and provide for effective contractual safeguards and commitments on technical and organisational measures.

---

101 See in this regard paragraph 2.10. and section 3.2.1. of this Decision..

102 See in this regard paragraphs 2.5. and 2.10., as well as section 3.2.3. of this Decision.

103 E.g. clause 11.2 of the contract.

5. The Court concludes the new *ad hoc* 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 *ad hoc* contractual clauses concluded by the Court.

6. The Court is to ensure that the provisions of the new *ad hoc* contractual clauses, including those in the main body of the contract[104], apply to and are binding upon other Cisco establishments (e.g. Cisco Inc. US), its affiliates, partners and sub-processors and are not rendered ineffective by the concurrent application of other obligations Cisco may impose on them (e.g. intra-corporate agreements).

7. The new *ad hoc* clauses must therefore 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.

8. If the other recipients do not adhere to the new *ad hoc* 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 is to satisfy itself that such measures implemented for transfers to other recipients: i) correspond to the role and the processing of transferred data the recipient will carry out and ii) are in line with the assessments made and supplementary measures identified by the Court during the TIA.

9. The new *ad hoc* 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 Cisco, its affiliates or its sub-processors receive from public authorities of a third country, or from another requesting third party in a third country, and to legally challenge such disclosure requests;

10. The new *ad hoc* contractual clauses include clauses whereby Cisco certifies that:
    (i) it has not purposefully created back doors or similar programming that could be used to access the system and/or personal data,
    (ii) it has not purposefully created or changed its business processes in a manner that facilitates access to personal data or systems, and
    (iii) that national law or government policy does not require the importer to create or maintain back doors or to facilitate access to personal data or systems or for the importer to be in possession or to hand over the encryption key.

[104] In particular e.g. clause 11.2(b) of the contract.

11. The new *ad hoc* contractual clauses include clear obligations and commitments that the technical supplementary measures of the use cases 1 and 3 of Annex 2 to the EDPB Recommendations 01/2020 and fulfilling the conditions for their effectiveness[105] are adopted for *all* the Webex videoconferencing communications, using state of the art end-to-end encryption technology.

12. The new *ad hoc* contractual clauses include clear obligations and commitments that either:

    (i) the technical supplementary measure of the use case 2 of the EDPB recommendations is fully applied in all personal data transferred to Cisco, using state-of-the-art pseudonymisation technologies, or
    (ii) a combination of technical and organisational measures (pseudonymization, access controls, special training module for administrators etc.) is adopted, so that Cisco effectively does not have access to personal data.

13. The new *ad hoc* contractual clauses include clear obligations and commitments that:

    (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 anonymized data needed for the resolution of the problem, while Cisco will delete these data upon resolution of the problem;
    (iii) apart from the data received by the Court SPoC, Cisco shall not have access to other Court data.

14. The new *ad hoc* contractual clauses need to ensure that specific training procedures for personnel in charge of managing requests for access to personal data from public authorities will be developed, that includes the requirements of EU law as to access by public authorities to personal data, in particular as following from Article 52 (1) of the Charter of Fundamental Rights. Such training should be periodically updated to reflect new legislative and jurisprudential developments in the third country and in the EEA.[106]

4.4. The Court is required to remedy the compliance issues identified in the present authorisation[107] to ensure an essentially equivalent level of protection within one year from the date of this Decision, following which the EDPS will reassess the transfer authorisation and may order the suspension of data flows.

[105] See in this regard paragraphs 90 and 94 of the EDPB Recommendations 01/2020.
[106] See paragraph 131 of the EDPB Recommendations 01/2020.
[107] See in particular under section 3 and paragraph 4.3. of this Decision.

4.3. Intermediate compliance progress report

4.5. The EDPS urges the Court to inform the EDPS without undue delay of any suspension by the Court of transfers of personal data under these *ad hoc* clauses pursuant to clause 5(a) or (b) of Annex 1d - Attachment B and of any revision or discontinuation of these *ad hoc* clauses pursuant to clause 11.2 or clause 19 of the main body of the contract or pursuant to clause 5(a) or (b) of Annex 1d - Attachment B.

4.6. The Court is to provide to the EDPS **an intermediate compliance report six months after the date of this Decision** demonstrating steps taken to implement the conditions set for the renewal of the authorisation. This report shall include information on progress on the commitments undertaken by the Court and those undertaken by Cisco.

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, 31 August 2021

[e-signed]

Wojciech Rafał WIEWIÓROWSKI