EDPS Decision on the Court of Justice of the EU's request to authorise the contractual clauses between the Court of Justice of the EU and Cisco Systems Inc. for transfers of personal data in the Court's use of Cisco Webex and related services

13 July 2023

(Case 2023-0367)

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 Regulation (EU) 2018/1725 (the 'Regulation')[1].

Given the Court's progress in its compliance with the conditions of the EDPS Authorisation Decision of 31 August 2021 and the EDPS Authorisation Decision of 28 October 2022, the EDPS finds that there are no transfers that fall under the scope of an authorisation under Article 48(3)(a) of the Regulation.

In the context of the present Decision, the EDPS has not carried our any investigation or on-the-spot checks or audit of the processing and flows of personal data in the Court's use of Cisco Webex and related services as they occur in practice and of the effectiveness of the technical and organisational measures implemented by the Court and Cisco.

The exercise of the EDPS powers in the present Decision is without prejudice to investigative and corrective powers of the EDPS, which may be relied on in a separate procedure to allow the EDPS to verify the factual assertions made by the exporting Union institutions, bodies, offices and agencies (EUIs) in the context of authorisation procedures under Articles 48(3)(a), 57(1)(e) and 58(3)(e) of the Regulation.

This Decision is not a general endorsement nor certification of data protection compliance of the videoconferencing services provided by any Cisco Webex entity.

[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.

Contents

I. PROCEEDINGS

1. This Decision concerns the request from the Court of Justice of the European Union ('the Court') for authorisation of contractual clauses under Article 48(3)(a) of Regulation (EU) 2018/1725[2] (the 'Regulation') to be concluded between the Court and Cisco Systems Inc., in the context of transfers of personal data in the Court's use of Cisco Webex and related services.[3]

2. The Court's use of Cisco Webex and related services generates multiple data flows. Based on the information provided to the EDPS by the Court, none of these data flows fall under the scope of an authorisation decision under Article 48(3)(a) of the Regulation.

3. As such, this Decision does not include in its scope transfers provided for under the contract between the Court and the UK company Cisco International Limited, which are effectively prevented by the Court, as described in points 21-26 of this Decision.

4. Similarly, this Decision does not include in its scope the transfers of personal data that are subject to Article 50(1)(d) of the Regulation, for which an authorisation for the EDPS is not required. Under Article 50(6) of the Regulation, the EDPS takes note of the categories of cases in which this Article is applied in the Court's use of Cisco Webex services, as described in points 40-55 of this Decision.

5. This Decision does not include in its scope transfers potentially resulting from unauthorised remote access, as described in points 29-39.

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

7. This Decision is addressed to the Court.

---

[2] 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.

[3] The Court concluded a contract (the Enterprise License Agreement - 'ELA') with Cisco International Limited UK, 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). This information was provided to the EDPS in the context of the EDPS Authorisation Decision of 31 August 2021.

II. BACKGROUND INFORMATION

A. Previous EDPS decisions

8. On 31 August 2021, the EDPS temporarily authorised the use of contractual clauses between the Court and Cisco Systems Inc. for transfers of personal data in the Court's use of Cisco Webex and related services ('EDPS Decision of 31 August 2021').[4] In that Decision, the EDPS set 14 conditions that the Court was required to meet for the renewal of the authorisation.[5]

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

10. On 28 October 2022, following an assessment of the Court's implementation report to the EDPS Decision of 31 August 2021, the EDPS extended temporarily and conditionally the authorisation to use the mentioned contractual clauses ('EDPS Decision of 28 October 2022').[6] In that Decision, the EDPS called on the Court to clarify several outstanding issues and to introduce further changes to the contractual obligations between the Court and Cisco Systems Inc.

11. The Court was required to ensure an essentially equivalent level of protection within 16 months after the date of the Decision of 28 October 2022, i.e. by 1 March 2024, by remedying the compliance issues identified in that Decision. The Court was also required to provide to the EDPS an intermediate compliance report 12 months after the date of that Decision, i.e., by 1 November 2023, demonstrating steps taken to implement the conditions set in that Decision.

12. On 22 May 2023, the Court submitted the following documents:
    - Final compliance report;
    - Redrafted draft Supplementary Agreement No. 1 to 'CISCO and Court of Justice of the European Union Enterprise License Agreement (ELA)', together with its
        - Exhibit A: ' Contractual Clauses' ('contractual clauses') with its
            - Annex 1a: 'Cisco Webex Meetings: Transfers of Personal Data',
            - Annex 1b: 'Cisco Technical Assistance ('TAC') Service Delivery: Transfers of Personal Data';
        - Exhibit B: 'List of Sub-processors';
        - Exhibit C: 'Information Security Exhibit';
        - Exhibit D: 'Data Privacy Sheets' with its
            - Attachment 1: 'Webex Meeting Privacy Data Sheet',
            - Attachment 2: 'TAC Privacy Data Sheet'.
    - Revised 'Data Transfer Impact Assessment for the Use of CISCO Webex by the Court of Justice of the European Union' ('Revised TIA') with Annexes:

[4] EDPS Authorisation Decision of 31 August 2021 (case 2021-0255).
[5] The conditions are listed under Section 3 of the EDPS Decision of 31 August 2021.
[6] EDPS Authorisation Decision of 28 October 2022 (case 2022-0902).

- Annex I: 'Videoconference Policy';
- Annex II: 'OSU Cisco TAC management procedure';
- Annex III: '*Registre des activités de traitement des données personnelles - Services de vidéoconférence et de communication unifiée*' and 'Information notice on the protection of personal data - Video Conferencing Services (Cisco Webex Meetings)'.

B. Facts

13. The EDPS explained its understanding of the contractual obligations between the Court and Cisco Systems Inc., and other Cisco entities in points 2.1.-2.6. of the EDPS Decision of 28 October 2022. These findings of fact are not being repeated here for the sake of brevity.

14. Based the submitted documents, **the EDPS understands the following as new or clarified facts**:

14.1. '**User-Generated Information'** refers to Meeting Recordings, Transcriptions of meeting recordings, Uploaded Files, which **include real-time meeting data** such as VoIP, video and high frame rate sharing data.[7]

14.2. The '**Webex Data Residency for EU countries'** programme, deployed by Cisco International Limited, is activated with regard to all of the Court's personal data and ensures that personal data processed by Cisco International Limited and its affiliates under its agreement with the Court is processed **in Frankfurt, Germany, with a back-up data centre in Amsterdam, The Netherlands**.[8] The Court verified the application of this choice through the Control Hub of Webex.[9]

14.3. The deployment of the Webex Data Residency programme for the Court's personal data, including real-time data, means that all processing operations, including storage, take place in the Court's geographic region mentioned in point 14.2. Based on assurances from Cisco International Limited[10] and the specific contractual obligations between the Court and Cisco International Limited[11], Cisco International Limited located in the UK **does not access the data of the Court by default**, and in any case does not access the data of the Court without explicit authorisation. In addition, **none of the Cisco sub-processors located outside of the European Economic Area (EEA) have a default remote access to the Court's data processed in the EEA**.

---

7 Point 2 of Annex 1a to Exhibit A to the Supplementary Agreement.
8 Article 1(4)(iii) of the Supplementary Agreement.
9 Point 26 of the Revised TIA.
10 Emails received by the Court from Cisco with clarifications concerning remote access received, transmitted to the EDPS on 13 and 17 February 2023 (registered in the internal EDPS case management system).
11 Article 4(4)(c) of the Supplementary Agreement (last paragraph on page 5 thereof). This paragraph incorporates the EDPS requirements under Condition 13 of the EDPS Decision of 31 August 2021.

III. LEGAL ANALYSIS

A. Nature of the authorisation under Article 48(3) of the Regulation

15. Under Article 46 of the Regulation, any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation shall take place only if, subject to the other provisions of the Regulation, the conditions laid down in Chapter V of the Regulation are complied with by the controller and processor, including for onward transfers of personal data from the third country or an international organisation to another third country or to another international organisation. All provisions in Chapter V of the Regulation shall be applied in order to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined.

16. In the absence of a decision pursuant to Article 45(3) of Regulation (EU) 2016/679[12] or to Article 36(3) of Directive (EU) 2016/680[13], a controller or processor may transfer personal data to a third country or to an international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available.

17. Subject to the authorisation from the EDPS, appropriate safeguards may be provided for by, in particular, contractual clauses between the controller or processor and the controller, processor or the recipient of the personal data in the third country or international organisation.[14]

18. The EDPS authorisations granted under Article 48(3)(a) of the Regulation have for their object such transmissions of personal data that qualify as transfers under the

[12] 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 or **GDPR**), OJ L 119, 4.5.2016, p. 1.

[13] 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 (**Law Enforcement Directive**), OJ L 119, 4.5.2016, p. 89.

[14] Article 48(3)(a) of the Regulation.

Regulation.[15] Observing the authorising nature of such EDPS decisions,[16] the EDPS in this role aims to check contractual compliance with the Regulation of the exporting EUIs. Under authorisation procedures, the EDPS does not carry out an investigation or on-the-spot checks and audit of the processing and flows of personal data in a EUI's use of a certain service as they occur in practice and of the effectiveness of the technical and organisational measures implemented by the EUI and the provider of that service. The scope of EDPS authorisations is limited to verifying that the contractual clauses between the controller and the processor with which the contract is concluded provide appropriate safeguards. This does not exempt the controller from fulfilling its obligations under Article 29 of the Regulation, including in relation to transfers.

19. The exercise of authorisation powers is without prejudice to investigative and corrective powers of the EDPS which may be relied on in a separate procedure to allow the EDPS to verify the factual assertions made by the exporting EUIs in the context of authorisation procedures under Articles 48(3)(a) and 58(3)(e) of the Regulation.

20. An authorisation decision issued by the EDPS is not a general endorsement nor certification of data protection compliance of the services provided by any entity of the provider.

B. Transfers subject to an EDPS authorisation

1. Transfers that could result from exceptions to the Data Residency Programme and measures to prevent such transfers from happening

21. In light of the facts presented in point 14.3, the EDPS finds that in the case at hand there is **no** disclosure by transmission or otherwise making personal data available by the Court to Cisco International Limited UK. It is because the latter is **contractually excluded** from having access to or accessing Court's personal data

[15] Since the Regulation introduces no legal definition of a 'transfer', the EDPS relies in particular on the cumulative criteria to qualify a processing operation as a transfer as identified by the EDPB Guidelines on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR, Version 2.0 adopted on 14 February 2023 ('**EDPB Guidelines 05/2021**').
In the interest of a coherent approach to personal data protection throughout the Union, and the free movement of personal data within the Union, the legislators aligned the Regulation as far as possible with the data protection rules adopted for the public sector in the Member States. In line with Recital 5 of the Regulation, whenever the provisions of the Regulation follow the same principles as the provisions of the GDPR, those two sets of provisions should, under the case law of the Court of Justice of the European Union, be interpreted homogeneously, in particular because the scheme of this Regulation should be understood as equivalent to the scheme of the GDPR. Consequently, the EDPS by analogy relies on guidance issued by the EDPB in the context of its interpretation of the Regulation where the interpreted provisions and principles, like in this case, are the same.

[16] As opposed to corrective and investigative powers of the EDPS under Article 58(1) and (2) of the Regulation.

located in the EEA.[17] In addition, based on the description in the documentation provided to the EDPS, technical measures such as **Zero Trust Security End-to-End encryption** effectively prevent Cisco's access to real time meeting data.[18] As such, the transmission of personal data by the Court to data centres located in the EEA under the Data Residency Programme does not meet all of the criteria identified by the European Data Protection Board (EDPB) that would qualify it as a transfer.[19] Considering **they are not transfers** in the sense of Chapter V of the Regulation, these processing operations are not included in the scope of this Decision under Article 48(3)(a) of the Regulation.[20] It follows that when the Webex Data Residency programme is deployed for the personal data in Court's use of Cisco Webex services, there are no transfers of personal data.

22. While there are contractual exceptions to the deployment of the Webex Data Residency programme because of '*specific actions or use of functions by the user administrator or user*'[21], as a result of which transfers of personal data may take place, the EDPS considers that, based on the information provided, **the Court has mitigated their application in a way that effectively prevents the transfers from taking place in the following manner**[22]:

Description of an exception to Webex Data Residency[23]	**Mitigating measures introduced by the Court**
Customer or user registers a user on any Cisco platform (for example, through www.webex.com or www.cisco.com) or	The users of the Court do not need to register themselves on any Cisco platform or a Cisco service in order

[17] Section 6 of Annex 1a to Exhibit A to the Supplementary Agreement as well as point 25 of the Final Compliance Report where the Court certifies that '*access to data stored in the EEA by the Supplier, i.e., Cisco International Limited, and its sub-processors has been contractually excluded under Art. 1(4)(c)(second last paragraph) of the Supplementary Agreement and confirmed by Cisco through clarifications provided in emails to the CJEU of 13 and 17 February 2023.*'

[18] For description of its functioning see section 3.1.10 of the EDPS Authorisation Decision of 28 October 2022. The EDPS notes that the Court updated its documentation and information notice to be provided internally and externally, including technical requirements for the use of Zero Trust Security End-to-End encryption. This documentation was provided to the EDPS as Annex III to the Revised TIA.

[19] The EDPB has identified three cumulative criteria to qualify a processing operation as a transfer in its Guidelines 05/2021, point 9 (see footnote 15). In the case at hand, condition 2 is not fulfilled because there is no disclosure by transmission or otherwise making available of data.

[20] Even if one was to consider that condition 2 of the EDPB Guidelines 05/2021 is fulfilled, the EDPS notes that these transmissions would take place to the UK that is covered until 27 June 2025 by the adequacy decision under Article 45 of the GDPR and therefore such transfers would have to comply with Article 47 of the Regulation. It follows that even if these transmissions were qualified as transfers, they would not fall under the scope of this Decision under Article 48(3)(a) of the Regulation.

[21] Section 6 of Annex 1a to Exhibit A to the Supplementary Agreement.

[22] As regards exceptions to the Data Residency Program resulting from (i) a user making a technical assistance request to the Cisco Technical Assistance Center and (ii) the Court providing ordering information to Cisco, see respectively Sections C.2.and C.3. of this Decision.

[23] Para 45 of the Revised TIA, page 24 of Annex 1a to Exhibit A and Point 4 of Attachment 1 to Exhibit D.

through any Cisco service to learn more about Cisco products or events	to use Webex. External users are also not required to perform such a registration.[24]
A user engages in collaboration with users outside of the EU region	The Court deactivated the option Global Distributed Meetings, as a result of which data transfers do not take place when there is a collaboration with users outside of the EEA region.[25] The processing operations take place on media nodes located in the EEA. Webex Meetings users located out of the EEA and participating in a videoconference organised by the Court connect to a media node located in the EEA.
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).	The Court blocks optional functionalities that might necessitate a transfer of personal data without appropriate safeguards.[26] In addition, the Court requires that only professional devices be used for work related communications, and explained *that these devices have 'push' notifications disabled at default.*[27]

23. The EDPS considers that the use of the **Webex Zero Trust Security End-to-End**, applicable to the User Generated Data[28], is one of several technical measures significantly contributing to the integrity and confidentiality of processing operations under Article 4(1)(g) of the Regulation, as well as the security and confidentiality of electronic communications, systems and networks Article 36 of the Regulation.[29]

24. In addition, the Court introduced **additional organisational measures** aimed at limiting the transmission of personal data. With regard to User Information: for the

[24] Paras 132(a) and 143 of the Revised TIA.
[25] Point 6 of Annex 1a to Exhibit A.
[26] Para 132(e) of the Revised TIA.
[27] Para 132(f) of the Revised TIA. The Court has provided the EDPS with copies of its internal policies that confirm that such instructions are given to its staff – attachment to the revised TIA *titled Lignes directrices relatives aux communications électroniques à la Cour de justice de l'Union européenne*, adopted on 13 December 2021.
[28] Point 3.72 of the EDPS Authorisation Decision of 28 October 2022.
[29] For description of its functioning see section 3.1.10 of the EDPS Authorisation Decision of 28 October 2022.

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 Security Assertion Markup Language ('SAML') protocol. Hence, 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.[30]

25. 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 Voice Over Internet Protocol only, which avoids transmission of phone numbers to conduct a Webex meeting.[31]

26. Based on the information provided, the EDPS considers that the measures that the Court has introduced effectively prevent the chance that the contractual exceptions to the Webex Data Residency are triggered. As a result, **even though transfers remain foreseen under the ELA between the Court and Cisco Systems Inc., the Court's additional internal measures effectively prevent such transfers from taking place**. It follows that in these circumstances there are no transfers which would require an authorisation under Article 48(3)(a) of the Regulation.

2. Conditions of EDPS Authorisation Decision of 28 October 2022

27. Based on the Final Compliance Report, the EDPS' understanding of facts under points 13 and 14 above and considering that some (possible) transfers are not subject to an EDPS authorisation[32], the EDPS finds that the **Court complied with all the conditions** imposed in the EDPS Authorisation Decision of 28 October 2022.

28. In relation to **Condition 6** of the EDPS Authorisation Decision of 28 October 2022 as regards the relevance of compliance with Protocol No. 7 to the Treaties on the Privileges and Immunities of the European Union (the 'Protocol')[33], the EDPS concludes the following: the protections afforded by the Protocol extend to personal data contained in the archives of the EUIs insofar as such archives contain personal

[30] Point 143 of the Revised TIA.
[31] Point 143 of the Revised TIA.
[32] See below Section C. Transfers not subject to an EDPS authorisation.
[33] Condition 6 of the EDPS Authorisation Decision of 28 October 2022 reads as follows: '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'.

data.[34] The high level of protection that Article 16 TFEU and Article 8 of the Charter afford to personal data include, whenever applicable, the protection afforded by the Protocol insofar as inviolable archives of the Union contain personal data. In that sense, **Article 8 of the Charter should be interpreted in conformity with the provisions on the secrecy of Union archives in Article 2 of the Protocol in order to protect against disclosure of personal data which are part of such archives**. The assessment of the compliance with the Protocol is however not required for the purposes of this Decision. Nevertheless, the EDPS recommends that the Court consider the provisions on the secrecy of Union archives in Article 2 of the Protocol.

C. Transfers not subject to an EDPS authorisation

1. Possible non-EU/EEA governmental access requests

29. In the EDPS Authorisation Decision of 28 October 2022, the EDPS stressed that '[e]*ven 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.*[35] The EDPS required that the Court assess, and if finds to be present, properly mitigate, the risk of unauthorised disclosure as a result of third-country laws with extra-territorial reach.[36]

30. Following the additional explanations provided by the Court, in particular in revised documents submitted on 22 May 2023[37], the EDPS has reassessed the above risk in relation to both the applicable legal framework (i), and the circumstances of the case (ii).

(i) Applicability of Chapter V of the Regulation to merely potential transfers and obligations to ensure integrity and confidentiality of personal data against risks of remote access.

31. According to the EDPB[38], a processing operation may be qualified as a transfer when three cumulative criteria are met: (1) a controller or a processor ('exporter') is subject to the GDPR for the given processing, 2) the exporter discloses by transmission or otherwise makes personal data, subject to this processing, available to another controller, joint controller or processor ('importer'), and 3) the importer is in a third

[34] CJEU, 17 December 2020, Commission v. Slovenia, C-316/19, ECLI:EU:C:2020:1030, para 73-75 and 78.
[35] Point 3.9 of the EDPS Authorisation Decision of 28 October 2022.
[36] Ibid.
[37] See point 12 of this Decision.
[38] As indicated above (footnote 15), the EDPS by analogy relies on guidance issued by the EDPB in the context of its interpretation of the Regulation where the interpreted provisions and principles, like in this case, are the same

country, irrespective of whether or not this importer is subject to the GDPR for the given processing in accordance with Article 3, or is an international organisation.[39]

32. The EDPS finds that for transfers meeting the three cumulative criteria and which are envisaged under a contract, i.e., transfers that the controller knows or should foresee in the broader context of the execution of the contract, or under other organised relationship, a transfer tool under Chapter V of the Regulation must be relied upon before any such transfers occur.

33. In that vein, remote access from a third country constitutes a transfer when it happens if the three above-mentioned criteria are met.[40] Equally, remote governmental access under third-country laws to personal data located and processed in the EEA, when it takes place, results in transfers of personal data.[41]

34. However, in the EDPS opinion, the mere risk that remote access by third country entities to data processed in the EEA may take place, does not constitute a transfer subjected to Chapter V of the Regulation.

35. The EDPS considers that transfers resulting from unauthorised access by third country entities, which are merely potential and in no way foreseeable in light of the content or purpose of a contract or another stable relationship between the parties, do not fall under the scope of Chapter V of the Regulation. The unlikely and unplanned character of such risks of such unauthorised access renders them unsuitable to be *ex ante* subjected to regime of Chapter V of the Regulation. It follows that for such potential and unplanned transfers a transfer tool under that Chapter is not required.

36. The EDPS recalls that the risks of such potential transfers resulting from the application of third-country laws to processors located in the EEA must be part of controller's analysis and assessment in line with the principle of accountability.[42] Before engaging a processor, the controller must assess the possible application of third country extra-territorial laws in order to ensure that, as required by Article 29 of the Regulation, it only uses processors providing sufficient guarantees to implement appropriate technical and organisational measures so that the processing is in line with the Regulation.[43] Where the processor complies with a disclosure request in violation of the controller's instructions and thus Article 29 of the Regulation, that processor shall be, in line with Article 29(10) of the Regulation, considered an independent controller of that processing.

---

[39] EDPB Guidelines 05/2021, point 9.

[40] EDPB Guidelines 05/2021, point 16.

[41] By analogy see point 24 of the EDPB Guidelines 05/2021.

[42] See also Section 3.6 'Risk of access by foreign governments when using non-EU CSPs storing data in the EEA' of the 'EDPB report '2022 Coordinated Enforcement Action Use of cloud-based services by the public sector' adopted on 17 January 2023.

[43] By analogy, see point 24 of the EDPB Guidelines 05/2021. See also Section 5 'Points for attention for public bodies', in particular page 32, of the EDPB Report on the 2022 Coordinated Enforcement Action.

37. When concluding contractual arrangements and providing instructions to the processor in line with Article 29 of the Regulation, particular attention should be paid to the observance of the principles of integrity and confidentiality under Article 4(1)(f), and the related Articles 33 and 36 of the Regulation laying down requirements for security of the processing operations and security and confidentiality of electronic communications, systems and networks.

(ii) Assessment of the processing operations relevant for the present Decision

38. In the case at hand, transfers resulting from possible remote governmental access to data located in the EEA, while theoretically possible under the laws of the United States[44], are not envisaged nor planned under the contract between the Court and Cisco International UK. In that sense, the Court does not plan for such transfers to take place in the broader context of the execution of that contract or its stable relationship with Cisco Webex entities.

(iii) Conclusion

39. Based on the above, **the potential transfers of data located in the EEA data centres resulting from the application of third-country laws are not covered by Chapter V of the Regulation**, **and the Court does not need to provide for appropriate safeguards for them by means of contractual clauses**.[45] As such, the EDPS does not include these transfers in the scope of this Decision under Article 48(3)(a) of the Regulation.

2. Processing for the Court's use of Cisco Technical Assistance Service Delivery

40. One of the exceptions to the Data Residency Program, mentioned in point 22 above, is when a user makes a technical assistance request to the Cisco Technical Assistance Center ('TAC'). As a result, transfers to the United States of personal data included in the TAC Support Information[46] and Customer Case Attachment[47] take place.[48] In order to provide support, Cisco can also access and process User Information as well as Host and Usage Information.[49]

---

[44] Point 3.11 of the EDPS Authorisation Decision of 28 October 2022.

[45] However, should Cisco or any sub-processors receive a request from a third country for access or disclosure of data in the Court's use of Cisco Webex services and the Court intends to positively respond to such a request, the Court must ensure that such a transfer pursuant to the access request complies with Chapter V of the Regulation.

[46] Categories of personal data: name, email address, phone number of the employee appointed to open the service request, authentication information (exclusive of passwords), work organization and responsibilities, current employer name (see point A.2 to Annex 1b to Exhibit A to the Supplementary Agreement).

[47] Personal data contained in Customer Case Attachments depend on what is included those Attachments by the customer (see point A.2 to Annex 1b to Exhibit A to the Supplementary Agreement).

[48] Points 22 and 66 of the Revised TIA.

[49] Point 63 of the Revised TIA.

41. According to the Court, the use of TAC support leads to the processing of TAC Support Information and the Customer Case Attachments that both include personal data. In any case, to provide support, Cisco can access and process User Information as well as Host and Usage Information.[50] 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.

42. The Court took organisational measures to limit or avoid transfers of personal data outside of the EU/EEA in the context of TAC requests. In the adopted and distributed internal policy to its staff members, the Court laid down the procedure to be followed should support be needed in staff's use of Cisco Webex services.[51] First, no user can directly open a support case with Cisco. Any support request must be first directed to **the internal help desk (single point of contact) of the Court**, which provide a first level of support to Court's staff. Should this first level of support provided by the internal help desk not suffice, the request is transferred to the second layer of support, i.e. **Court's network engineers**. Should any problem related with the infrastructure need an escalation to the Cisco TAC support service, this activity is organised and done respecting the following rules:
    - Only the authorized Court network engineers can introduce support requests to the Cisco TAC service. No personal data relating to the problem is provided to Cisco TAC.
    - The requests shall be sent to Cisco during the normal Luxembourg working hours (8h-19h).
    - If further Court data is requested by the Cisco TAC service, the information requested should be analysed to determine if it contains personal data.
    - In case personal data is involved, the Court network responsible, the Court's DPO and the SSI service shall be informed.
    - The Court network engineers, in collaboration with the DPO, shall analyse the content of the data and the measures to be taken in order to ensure the protection of personal data.
    - In case Cisco needs to have remote access to the Court's Cisco Webex infrastructure, the DPO of the Court, in collaboration with the Court network engineers, shall analyse the possible risks for the data subjects and decide on the legitimacy of this access.

43. The EDPS understands that in practice the number of TAC requests initiated by the Court does not exceed to 2-3 tickets per year[52] and only takes place where the internal Court services cannot solve the issue itself.

---

[50] Ibid.

[51] Annex II to the revised TIA titled 'OSU Cisco TAC management procedure'; it was made available to the Court's staff members on 31 January 2023.

[52] Assertions made by the Court's representatives, including the DPO, during an internal meeting at the EDPS premises of 25 November 2021.

44. With regard to technical safeguards, the Court confirmed that TAC Support Information and Customer case attachments are only accessed by Cisco staff, and that no personnel from third-party service providers have access to this data.[53] The TAC Support Information is encrypted in transit, while Case Attachments are encrypted both in transit and at rest, in order to secure personal data from accidental loss and unauthorised access, use, alteration, and disclosure.[54] The keys for encryption are managed by Cisco.[55]

45. The EDPS considers that the Court transfers personal data, whether by electronic transmission or by making it available to Cisco Systems Inc., for the provision of technical support, and that this data is not effectively pseudonymised nor encrypted because the processing requires accessing data in the clear.[56] Based on his understanding of facts, the EDPS is of the opinion that the residual sets of transfers resulting from TAC requests cannot be covered by appropriate safeguards, despite reasonable efforts of the Court to provide for organisational and technical measures vis-à-vis unlikely and small risks of such transfers to data subjects' rights and freedoms. It follows that in these circumstances the Court is unable to provide for appropriate safeguards in the form of contractual clauses because effective supplementary measures are not conceivable without undermining the aim of the providing TAC support. Therefore, these transfers do not fall in the scope of this Decision under Article 48(3)(a) of the Regulation.

46. However, having regard to the need for the Court to dispose of stable services provided by Cisco in order to perform its tasks in the public interest, as well as the safeguards put in place, the EDPS is of the opinion that these transfers resulting from TAC requests can take place in accordance with Article 50, notably by relying on Article 50(1)(d) of the Regulation.

47. Article 50(1) of the Regulation provides that in the absence of an adequacy decision pursuant to Article 45(3) of GDPR or to Article 36(3) of the Law Enforcement Directive, or of appropriate safeguards pursuant to Article 48 of this Regulation, a transfer or a set of transfers of personal data to a third country or an international organisation shall take place only where specific conditions are met. Point d) of Article 50(1) lists one of these conditions, namely 'when the transfer is necessary for important reasons of public interest'. Such public interest shall be recognised in Union law.[57]

48. In parallel to what is provided for in Article 49 of the GDPR[58], derogations under Article 50 of the Regulation are exemptions from the general principle that personal

---

[53] Para 67 of the Revised TIA.
[54] Para 93 of the Revised TIA.
[55] Point 5 of the Court's answer of 15 September 2022.
[56] See Use Case 6 of the EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, adopted 18 June 2021 ('**EDPB Recommendations 01/2020**').
[57] Article 50(3) of the Regulation.
[58] See footnote 15.

data may only be transferred to third countries or international organisations if an adequate level of protection is provided for in the third country or international organisation or if appropriate safeguards have been adduced and the data subjects enjoy enforceable and effective rights in order to continue to benefit from their fundamental rights and safeguards.[59] Due to this fact and considering that Article 50 of the Regulation must be interpreted in accordance with the Charter[60], derogations can apply only in so far as is strictly necessary and must be narrowly construed.[61] Derogations must also be interpreted restrictively so that the exception does not become a rule.[62] This is also supported by the wording of the title of Article 50 which states that derogations are to be used for specific situations ('Derogations for specific situations').[63]

49. When considering transferring personal data to third countries or international organizations, data exporters should therefore favour solutions that provide data subjects with a guarantee that they will continue to benefit from the fundamental rights and safeguards to which they are entitled as regards processing of their data once this data has been transferred. As derogations do not provide adequate protection or appropriate safeguards for the personal data transferred and as transfers based on a derogation are not required to have any kind of prior authorisation from the supervisory authorities, transferring personal data to third countries on the basis of derogations leads to increased risks for the rights and freedoms of the data subjects concerned.[64]

50. The derogation of Article 50(1)(d) of the Regulation requires that the transfer of personal data is necessary for important reasons of public interest recognised in Union law. In the first place, the data exporter must identify and document **the existence of such 'public interest'**. Examples of public interest may include management and functioning of the EUIs[65], or public security or health[66]. The identified public interest must be explicitly '**recognised**' in '**Union law'**, which encompasses EU primary laws, general principles of EU law, international agreements recognising a certain objective or providing for international cooperation to foster that objective (as long as EU and/or the Member States are party to these agreements[67]), EU secondary laws, case law of the Court of Justice of the EU, as well as internal rules of the EUIs as long as they meet the requirements to be considered 'Union law' under Recital 23 of the Regulation.

---

59 EDPB Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679 ('**EDPB Guidelines 2/2018**'), page 4.

60 CJEU, 13 May 2014, Google Spain and Google, C-131/12, ECLI:EU:C:2014:317, para 68 and case-law cited.

61 CJEU, 11 December 2014, František Ryneš, C-212/13, ECLI:EU:C:2014:2428, paras 28-29 and case-law cited.

62 EDPB Guidelines 2/2018, page 4.

63 Ibid.

64 EDPB Guidelines 2/2018, page 4.

65 Recital 22 of the Regulation.

66 Recital 69 and Article 25(1)(a) of the Regulation.

67 EDPB Guidelines 2/2018, page 10.

51. As any processing operation, such as a transfer, is an interference with the fundamental rights, provisions of Article 50 of the Regulation must be interpreted in light of the Charter, in particular its Article 52(1). Therefore, in the second place, the data exporter must assess and document whether the planned transfer of personal data respects **the essence of the rights and freedoms** that the transfer interferes with, and whether the planned transfer is in accordance with the **principles of proportionality and necessity**. In other words, the data exporter must satisfy itself that it is necessary to process the personal data in question to attain the identified important public interest and that there are no less intrusive measures which would be comparably effective[68], as well as that, on balancing of interests, the identified public interest is important enough to justify the interference in question.[69] As part of that analysis, the data exporter must consider, inter alia, the categories of personal data transferred and of data subjects, character (e.g., large-scale[70]) and regularity of the transfers (systematic[71], or occasional and non-repetitive). Article 50(1)(d) of the Regulation may not be relied on for transfers that are both large-scale and systematic.[72]

52. In the case at hand, the EDPS finds that there is a public interest of ensuring management and functioning of the Court, as also confirmed by Recital 22 of the Regulation: being auxiliary to the main service of video-conferencing, technical assistance support is a quintessential element for proper functioning of video-conferencing software in line with state-of-the-art integrity and security standards. In turn, having a properly functioning video-conferencing tool has become indispensable to the daily functioning of the EUIs, such as the Court, as it allows for remote communication of staff members working from home.

53. Further, there is no alternative measure which would be less intrusive to the rights and freedoms of data subjects, and which would be comparably effective to the current set-up of TAC requests at the Court. Considering that, based on the information provided, the processing operations involve limited categories of personal data, transfers are very rare and affect very limited number of data subjects, **the Court may rely for transfers resulting from TAC requests on the**

---

[68] See Step 4 of steps to be followed are described in 'Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit'.

[69] See 'Checklist for assessing proportionality of new legislative measures', p. 12-33, in EDPS Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data.

[70] Article 29 Working Party ('WP29') indicated that the following factors should in particular be consider when determining if a processing operation is 'large-scale': the number of data subjects concerned - either as a specific number or as a proportion of the relevant population, the volume of data and/or the range of different data items being processed, the duration, or permanence, of the data processing activity, the geographical extent of the processing activity (see WP29 Guidelines on Data Protection Officers, endorsed by the EDPB, p. 8).

[71] Transfers are systematic when they regularly occur within a stable relationship (see EDPB Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679, p. 9). WP29 defined 'systematic' as meaning one or more of the following: occurring according to a system, pre-arranged, organised or methodical, taking place as part of a general plan for data collection, carried out as part of a strategy (see WP29 Guidelines on Data Protection Officers, endorsed by the EDPB, p. 9).

[72] EDPB Guidelines 2/2018, page 11.

derogation provided for under Article 50(1)(d) and (3) of the Regulation. It follows that such transfers do not fall within the scope of the present Decision.

3. Transfers of business customer information

54. One of the exceptions to the Data Residency Program, mentioned in point 22 above, is when a Customer, i.e., the Court, provides ordering information (business contact information). The Court explained that the ordering information is handled in the contract between the Court and Cisco International Limited UK. No further business contact information is required for the use of Webex services by the Court.[73] Personal data transferred are the name and surname of the representative of the Court empowered to enter into the contract, as well as names, surnames and email addresses of Court's contacts for service management and technical matters. That data may be handled at a Cisco data centre in any location, and certainly is transferred to the United States.

55. Similar to the reasoning in points 49-53 above, the EDPS is of the opinion that Recital 22 of the Regulation recognises the public interest of the Court in concluding and managing contracts for necessary services that are linked with the management of that institution. Likewise, there is no alternative measure which would be less intrusive to the rights and freedoms of data subjects, and which would be comparably effective. Considering that, based on the information provided, the processing operations involve very limited categories of personal data, transfers are very rare and affect very limited number of data subjects, **the Court can, for transfers resulting from contract management, make use of the derogations provided for under Article 50(1)(d) and (3) of the Regulation. It follows that such transfers do not fall within the scope of the present Decision.**

IV. CONCLUSION

56. Pursuant to Article 58(3)(e) of the Regulation, the EDPS finds that there are no transfers of personal data that would fall under the scope of an authorisation decision of contractual clauses referred to in Article 48(3)(a) of the Regulation.

57. This Decision **is without prejudice to EDPS' investigative and corrective powers** under Article 58 of the Regulation.

Done at Brussels, 13 July 2023

Wojciech Rafał WIEWIÓROWSKI

(e-signed)

[73] Point 132 b) of the Revised TIA.