EUROPEAN DATA PROTECTION SUPERVISOR

EDPS INVESTIGATION INTO USE OF MICROSOFT 365 BY THE EUROPEAN COMMISSION (Case 2021-0518)

Decision

(8 March 2024)

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

EXCERPT OF FINDINGS OF INFRINGEMENTS

AND OF USE OF CORRECTIVE POWERS

Purpose limitation

I. The EDPS finds that the Commission, on 12 May 2021 (the 'reference date') and continuously thereafter until the date of issuing this decision:

a) has infringed Article 4(1)(b) of Regulation (EU) 2018/1725 (the 'Regulation') by failing to:

- sufficiently determine the types of personal data collected under the 2021 ILA in relation to each of the purposes of the processing so as to allow those purposes to be specified and explicit;

- ensure that the purposes for which Microsoft is permitted to collect personal data under the 2021 ILA are specified and explicit;

b) has infringed Article 29(3)(a) of the Regulation by insufficiently determining in the 2021 ILA which types of personal data are to be processed for which purposes and by failing to provide sufficiently clear documented instructions for the processing;

c) has infringed Articles 4(2) and 26(1) in conjunction with Article 30 of the Regulation by failing to ensure that Microsoft processes personal data to provide its services only on documented instructions from the Commission;

d) has infringed Article 6 of the Regulation by failing to assess whether the purposes for further processing are compatible with the purposes for which the personal data have initially been collected;

e) has infringed Article 9 of the Regulation by failing to assess whether it is necessary and proportionate to transmit the personal data to Microsoft Ireland and its sub-processors (including affiliates) located in the EEA for a specific purpose in the public interest.

International transfers

II. The EDPS finds that the Commission, on the reference date and, except with regard to point b), second indent, and to point c),[1] continuously thereafter until the date of issuing this decision:

a) has infringed Article 29(3)(a) of the Regulation by failing to clearly provide in the 2021 ILA what types of personal data can be transferred to which recipients in which third country and for which purposes, and to give Microsoft documented instructions in that regard;

[1] With regard to point b), second indent, and point c), until the entry into force of the US adequacy decision.

b) has infringed Articles 4(2), 46 and 48 of the Regulation by failing to provide appropriate safeguards ensuring that personal data transferred enjoy an essentially equivalent level of protection to that in the EEA since it:

- has not appraised, either prior to the initiation of the transfers or subsequently, what personal data will be transferred to which recipients in which third countries and for which purposes, thereby not obtaining the minimum information necessary to determine whether any supplementary measures are required to ensure the essentially equivalent level of protection and whether any effective supplementary measures exist and could be implemented;

- had not implemented effective supplementary measures for transfers to the United States taking place prior to the entry into force of the US adequacy decision, in light of the *Schrems II* judgment, nor has it demonstrated that such measures existed;

c) has infringed Articles 4(2), 46 and 48(1) and (3)(a) of the Regulation by:

- concluding the SCCs for transfers from the Commission to Microsoft Corporation without having clearly mapped the proposed transfers, concluded a transfer impact assessment and included appropriate safeguards in those SCCs;

- failing to obtain authorisation of those SCCs for transfers from the Commission to Microsoft Corporation from the EDPS pursuant to Article 48(3)(a) of the Regulation;

d) has infringed Article 47(1) of the Regulation read in the light of Articles 4, 5, 6, 9 and 46 by failing to ensure that transfers take place "*solely to allow tasks within the competence of the controller to be carried out.*"

Unauthorised disclosures

III. The EDPS finds that the Commission, on the reference date and continuously thereafter until the date of issuing this decision:

a) has infringed Article 29(3)(a) of the Regulation, in particular as interpreted in the light of the *Schrems II* judgment, by not ensuring that, for personal data processed in the EEA, only EU or Member State law prohibits notification to the Commission of a request for disclosure, and that, for personal data processed outside the EEA, any prohibition of such notification constitutes a necessary and proportionate measure in a democratic society respecting the essence of the fundamental rights and freedoms recognised by the Charter;

b) has infringed Articles 4(1)(f), 33(1) and (2) and 36 of the Regulation, by:

- not having assessed the legislation of all third countries to which personal data are envisaged to be transferred under the 2021 ILA and thereby failing to ensure that Microsoft and its sub-processors do not make disclosures of personal data within and outside of the EEA that are not authorised under EU law;

- failing to implement effective technical and organisational measures that would ensure processing in accordance with the principle of integrity and confidentiality within the EEA and, as part of an essential equivalence of the level of protection, also outside of the EEA.

Use of corrective powers

IV. The EDPS has decided to take the following corrective measures in respect of the infringements detailed in sections 3.1.3, 3.2.3 and 3.3.3 of the decision:

1.1. to order the Commission, under Article 58(2)(j) of the Regulation and with effect from 9 December 2024, to suspend all data flows resulting from its use of Microsoft 365 to Microsoft and to its affiliates and sub-processors, located in third countries not covered by an adequacy decision as referred to in Article 47(1) of the Regulation, and to demonstrate the effective implementation of such suspension (*infringements set out in paragraphs II.a and b, first indent, and III*);

1.2. to order the Commission, under Article 58(2)(e) of the Regulation, to bring the processing operations resulting from its use of Microsoft 365 into compliance, and to demonstrate such compliance, by 9 December 2024, by:

1.2.1. carrying out a transfer-mapping exercise identifying what personal data are transferred to which recipients in which third countries, for which purposes and subject to which safeguards, including any onward transfers (*infringements set out in paragraph II.a and b, first indent*);

1.2.2. ensuring that all transfers to third countries take place solely to allow tasks within the competence of the controller to be carried out *(infringement set out in paragraph II.d*);

1.2.3. ensuring, by way of contractual provisions concluded pursuant to Article 29(3) of the Regulation and of other organisational and technical measures, that:

a) all personal data are collected for explicit and specified purposes (*infringements set out in paragraph I.a and b)*;

b) the types of personal data are sufficiently determined in relation to the purposes for which they are processed (*infringements set out in paragraph I.a and b)*;

c) any processing by Microsoft or its affiliates or sub-processors is only carried out on the Commission's documented instructions, unless, for processing within the EEA, required by EU or Member State law, or, for processing outside of the EEA, third-country law that ensures a level of protection essentially equivalent to that in the EEA, to which Microsoft or its affiliates or sub-processors are subject (*infringements set out in paragraphs I.b and c, II.a and III)*;

d) no personal data are further processed in a manner that is not compatible with the purposes for which the data are collected, in accordance with the criteria laid down in Article 6 of the Regulation (*infringement set out in paragraph I.d)*;

e) any transmissions to Microsoft Ireland or its affiliates and sub-processors located in the EEA comply with Article 9 of the Regulation (*infringement set out in paragraph I.e*);

f) for personal data processed in the EEA, only EU or Member State law prohibits notification to the Commission of a request for disclosure, and, for personal data processed outside the EEA, any prohibition of such notification constitutes a necessary and proportionate measure in a democratic society respecting the essence of the fundamental rights and freedoms recognised by the Charter, as required by Article 29(3)(a) of the Regulation, in particular as interpreted in light of the *Schrems II* judgment (*infringement set out in paragraph III.a*);

g) no disclosures of personal data by Microsoft or its sub-processors take place, unless, for personal data processed within the EEA, the disclosure is required by EU or Member State law, or, for personal data processed outside of the EEA, the disclosure is required by third-country law that ensures a level of protection essentially equivalent to that in the EEA, to which Microsoft or its affiliates or sub-processors are subject (*infringements set out in paragraph III.b*).

1.3. to issue a reprimand to the Commission under Article 58(2)(b) of the Regulation (*all infringements*).

Contents

The European Data Protection Supervisor,

Having regard to the Treaty on the Functioning of the European Union,

Having regard to Regulation (EU) 2018/1725, and in particular Article 57(1)(f) and Article 58(2)(b), (e) and (j) thereof,

Has issued the following decision:

1. INTRODUCTION AND SCOPE

1. This decision is issued following the EDPS' investigation into the European Commission's (the 'Commission') use of Microsoft 365 under the Inter-institutional Licensing Agreement signed on 7 May 2021 (the '2021 ILA').[2] The EDPS has conducted this investigation pursuant to Articles 57(1)(f) and 58(1)(b) of Regulation (EU) 2018/1725 (the 'Regulation').[3]

2. The objective of the investigation has been to examine whether the Commission's use of Microsoft 365 complies with the Regulation, including any processing carried out on its behalf.

3. The reference date for the purposes of establishing an infringement by the Commission is 12 May 2021 (the 'reference date'). This is the date on which the EDPS launched its investigation and notified it to the Commission. The EDPS has taken the Commission's actions after that date into account for the purposes of deciding on corrective measures. To this end, the EDPS has established whether infringements have continued after the reference date, and in particular until the date of issuing this decision.

4. This decision concerns the Commission in its capacity as a controller for the processing of personal data in the context of its use of Microsoft 365. The EDPS is, however, aware that this decision could have consequences for the Commission in its capacity as the lead contracting authority for the procurement of Microsoft products and services by EU institutions, bodies, offices and agencies ('EU institutions and bodies').

5. The investigation at the basis of the present decision has a precedent. In 2019 and 2020, the EDPS carried out an investigation into the use of Microsoft products and services by EU institutions or bodies under the Inter-institutional Licensing Agreement signed in 2018 (the '2018 ILA'). The EDPS found a number of infringements of the Regulation. In March 2020, the EDPS issued findings and recommendations (the '2020 Findings and

[2] References to the 2021 ILA are to be understood as references to the 2021 ILA as signed on 7 May 2021, without any subsequent amendments, unless specified otherwise.

[3] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39).

Recommendations') to assist EU institutions and bodies in bringing those processing activities into compliance.[4] The EDPS launched the current investigation following indications that several of our most significant concerns had not been addressed.

6. The EDPS welcomes the improvements implemented by the Commission in the 2021 ILA in comparison with the 2018 ILA. In particular, the EDPS welcomes the clarification of the scope of Microsoft's obligations under the Regulation in its capacity as a processor. The EDPS also welcomes the introduction of detailed audit provisions which allow the Commission to scrutinise the processing activities that take place to provide online services and software.

7. Nonetheless, several substantial areas of non-compliance remain. This decision focuses on specific areas that are of particular concern given the Commission's status as a public service institution. The EDPS has decided to limit the focus of this decision in light of its limited resources and the need for expedience. The EDPS reserves the right to take other or further action in respect of issues not accorded detailed consideration in this decision.

8. This decision focuses on the following key concerns:

   – the Commission's compliance with the purpose limitation principle established by the Regulation;

   – its compliance with the provisions of the Regulation applying to international transfers, as interpreted in the *Schrems II* judgment,[5] and in particular with Chapter V of the Regulation; and

   – its compliance with provisions of the Regulation pertaining to unauthorised disclosures of personal data.

2. PROCEEDINGS

9. On 12 May 2021, the EDPS launched an investigation into the Commission's use of Microsoft 365 under the 2021 ILA under Articles 57(1)(f) and 58(1)(b) of the Regulation. The EDPS requested information and evidence under Article 58(1)(d) of the Regulation.

10. On 21 May 2021 and 15 October 2021, the Commission responded to the request for information and evidence.

11. On 23 November 2021, the EDPS held an evidence-gathering meeting with the Commission. During that meeting, the Commission provided additional information and clarifications in relation to the evidence it had provided on 15 October 2021.

12. On 4 April 2022, the EDPS requested further information and clarifications.

---

[4] Annexed to EDPS letter of 23 March 2020 to all EU institutions and bodies. See EDPS Public Paper on Outcome of own-initiative investigation into EU institutions' use of Microsoft products and services.

[5] *Facebook Ireland and Schrems (Schrems II)*, C-311/18, ECLI:EU:C:2020:559.

13. On 7 June 2022, the Commission responded to the EDPS' request of 4 April 2022.

14. On 31 January 2023, the EDPS issued a preliminary assessment which was made available to the Commission, as well as to Microsoft Ireland Operations Ltd ('Microsoft Ireland'). The purpose of the preliminary assessment was to present the entities concerned with the EDPS' preliminary findings of fact; an initial legal assessment of those findings, including any alleged infringements of the Regulation; and the corrective measures the EDPS envisaged taking. This allowed the Commission and Microsoft Ireland to exercise their right to be heard and aimed to ensure that the EDPS' findings of fact were correct and complete.

15. On 14 March 2023, the EDPS provided the Commission and Microsoft Ireland, at their request, with a list of documents falling within the scope of access to the file and informed them of the modalities of obtaining access. The Commission and Microsoft Ireland accessed the file on 17 and 15 March 2023, respectively.

16. On 25 and 26 May 2023, respectively, the Commission and Microsoft Ireland provided separately their written observations on the preliminary assessment. They each also requested to be heard orally.

17. On 28 July 2023, the EDPS announced the date of the hearing to the Commission and invited it to communicate to Microsoft Ireland that it may attend the hearing. On 14 September 2023, the EDPS informed the Commission of the modification of the date of the hearing due to logistical reasons.

18. On 27 September 2023, the EDPS informed the Commission and Microsoft Ireland of the Rules on the Hearing in EDPS' Investigations.[6] The EDPS also invited them to make known their views on a list of questions, in order to ensure the correct and complete understanding of their replies to the preliminary assessment.

19. On 23 October 2023, the EDPS held a hearing attended by the Commission and Microsoft Ireland. Its purpose was to allow the Commission and Microsoft Ireland to make their views on the preliminary assessment known orally.

20. On 19 December 2023, the Commission provided the EDPS with an amendment to the 2021 ILA which it had concluded with Microsoft Ireland on the same day.

21. The EDPS has taken into consideration all of the representations and evidence submitted by the Commission and Microsoft Ireland during the investigation, including in the written reply to the preliminary assessment and at the hearing. The EDPS has also taken into consideration information provided by Microsoft on its website, as well as, in so far as relevant, a number of reports issued by data protection authorities in the European Economic Area ('EEA') and by the Dutch Ministry of Justice. These reports are relevant in the present investigation because they concern the same or similar enterprise versions of Microsoft products to those used by the Commission under the 2021 ILA. In other words, those products are part of the Microsoft 365 software or its earlier versions. They also concern flows of the same or similar types of personal data to Microsoft for

[6] EDPS Decision of 27 September 2023 on the Rules on the Hearing in EDPS' Investigations.

essentially identical purposes in the use of those products. The processing with regard to such products is also governed by similar Microsoft licensing contractual documents.[7]

3. FINDINGS OF FACT AND OF LAW

Reference date

22. As noted in paragraph 3, the reference date for the purposes of establishing an infringement by the Commission is 12 May 2021. In this regard, Microsoft Ireland considers that any findings of infringements should not be based on the facts existing on the reference date.[8] Such findings should instead be based, in its view, on the latest information available to the EDPS and not what would constitute an "*arbitrarily selected*" historical date.[9] According to Microsoft Ireland, any findings of infringements that are based on "*outdated facts which are no longer applicable*" would "*needlessly harm the reputation and business of Microsoft*".[10] It considers that such findings would give a misleading impression that a "*current infringement*" has been found.[11]

23. Under Article 52(3) of the Regulation, the EDPS is responsible for monitoring and ensuring the application of the provisions of the Regulation. To that end, the EDPS, inter alia, conducts investigations on the application of the Regulation, as provided for in Article 57(1)(f) thereof. The EDPS also exercises its powers under Article 58 of the Regulation, including to issue reprimands where processing operations "*have infringed*"[12] provisions of the Regulation, as provided for in Article 58(2)(b) thereof. Therefore, the Regulation explicitly empowers the EDPS to issue reprimands also where the infringement is terminated at the time when such power is applied. In order to issue a reprimand, the EDPS must determine whether there has been an infringement, regardless of whether it has since ceased or not. A different interpretation is not compatible with the Regulation and would lead to an unwarranted pardon of breaches of the Regulation which often result in undue interferences with the fundamental right to protection of the personal data of the persons concerned.[13]

24. Furthermore, where an investigation is based on a complaint, it is well-established practice by the EDPS, in line with Article 16(4) of its Rules of Procedure,[14] and by other supervisory authorities under the GDPR[15] that the findings will relate to the event referred to in the complaint. Such an event may have taken place on a specific date or

---

7 See in this respect https://www.microsoft.com/licensing/terms and https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA.
See also https://www.microsoft.com/licensing/terms/product/PrivacyandSecurityTerms/EAEAS.

8 Reply by Microsoft Ireland of 26 May 2023, para. 130. See also para. 385.

9 Reply by Microsoft Ireland of 26 May 2023, paras. 42 and 131.

10 Reply by Microsoft Ireland of 26 May 2023, para. 135.

11 Reply by Microsoft Ireland of 26 May 2023, paras. 134.

12 And not e.g. "*is infringing*".

13 Cf. *Facebook Ireland*, C-645/19, Opinion of the Advocate General Bobek, ECLI:EU:C:2021:5, point 159.

14 Decision of the European Data Protection Supervisor of 15 May 2020 adopting the Rules of Procedure of the EDPS (OJ L 204, 26.6.2020, p. 49).

15 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).

period, or may still be ongoing at the time of the submission of the complaint. However, the fact that the controller takes measures that ensure that the infringement has ceased before the supervisory authority issues a decision on the complaint cannot result in the supervisory authority's inability to find an infringement.[16] Neither the Regulation nor the GDPR provide for such a limitation of the powers of supervisory authorities to the consequential detriment of the rights of data subjects. If the controllers considered that they can avoid any finding of infringement by merely ceasing the infringement during the investigation, they would undoubtedly be less inclined to proactively ensure compliance before any investigation is initiated. The EDPS sees no reasons to distinguish own-initiative investigations from complaint-based investigations in this regard.

25. The EDPS also rejects the claim that findings of infringements that took place in the past would needlessly harm Microsoft's reputation and business. Any reputational or similar damage that may occur would be an inherent consequence of non-compliance with the law and would be purely incidental to the lawful exercise of the EDPS' powers. Given that this decision specifies the period to which an infringement pertains, any "*misleading impression*" referred to by Microsoft Ireland can be avoided by an average reader and can therefore not be reasonably imputed to the EDPS.

Processing of personal data within the scope of the Regulation

26. The 2021 ILA constitutes the contractual basis for the Commission's use of Microsoft 365 on the reference date, and has since been amended several times, as noted in more detail below. As provided in the Master Business and Services Agreement (the 'MBSA'), which is an integral part of the 2021 ILA, all **processing** undertaken by Microsoft on behalf of the Commission for the purposes of providing its services is regulated by the Data Protection Addendum (the 'DPA').[17] The Commission and Microsoft Ireland have not disputed that the operations carried out on personal data under the 2021 ILA constitute processing of personal data within the meaning of Article 3(3) of the Regulation. This is also explicitly acknowledged throughout the 2021 ILA.[18]

27. The DPA defines various types of data processed under the DPA using Microsoft's typology ("C*ustomer Data*", "*Diagnostic Data*", "*Service Generated Data*", "*Professional Services Data*", "*Support Data*", "*Functional Data*").[19] The Commission and Microsoft Ireland acknowledge that all these types of data contain **personal data**.[20] They also recognise that: "*any Personal Data pseudonymized, or de-identified but not anonymized, or Personal Data derived from Personal Data is also Personal Data.*"[21] It is therefore the EDPS' understanding that personal data are processed in all service contexts. The Commission and Microsoft Ireland have not disputed that understanding in their written and oral

[16] Notwithstanding the fact that such measures by the controller may be taken into account by the supervisory authority when deciding how to handle a complaint and are to be taken into account when using corrective powers.

[17] Clause 4(b) of the MBSA, 2021 ILA, p. 5.

[18] See, for example, 2021 ILA, pp. 28-29.

[19] DPA's definitions, 2021 ILA, pp. 25-26. The Product Terms site, which also regulates the processing under the 2021 ILA, also refers to other types of personal data, such as "*required services data*".

[20] Section "*Processing of Personal Data; EUDPR*" in the main body of the DPA and the equivalent provisions in Chapters 2 and 4 of Attachment 1 of the DPA, 2021 ILA, pp. 30, 53 and 66.

[21] Section on "*Processing of Personal Data; EUDPR*" in the main body of the DPA, 2021 ILA, p. 30, and Chapter 2 of Attachment 1 to the DPA, 2021 ILA, p. 53.

submissions, except as regards certain data processed for Microsoft's own business operations. Those objections are analysed in section 3.1.2.3.

28. Article 2(1), in conjunction with Article 3(10), of the Regulation provides that it applies to the processing of personal data by all Union institutions, bodies, offices and agencies. The Commission is an EU institution under Article 13(1) of the Treaty on European Union. Moreover, it is a controller, within the meaning of Article 3(8) of the Regulation, for processing of personal data under the 2021 ILA.[22] Processing of personal data that it carries out as a controller therefore falls within the scope of the Regulation. This includes the processing that is carried out on its behalf by Microsoft Ireland as its processor, and its sub-processors (Microsoft Corporation and other sub-processors, including affiliates).[23]

3.1. Purpose limitation

3.1.1. Applicable law

29. Article 8(1) and (2) of the Charter of Fundamental Rights of the European Union (the 'Charter') provide that:

> *1. Everyone has the right to the protection of personal data concerning him or her.*
>
> *2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.*"

30. Article 16 of the Charter provides that:

> *The freedom to conduct a business in accordance with Union law and national laws and practices is recognised.*

31. Article 4(1)(b) of the Regulation provides that:

> *Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; [...] ('purpose limitation').*

32. Article 4(2) of the Regulation provides that:

> *The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1. ('accountability').*

33. Article 6 of the Regulation provides that:

> *Where the processing for a purpose other than that for which the personal data have been collected is not based on the data subject's consent or on Union law which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 25(1), the controller shall, in order to ascertain*

[22] 2021 ILA, pp. 26 and 30.
[23] See judgment in Case C-683/21, *Nacionalinis visuomenės sveikatos centras*, ECLI:EU:C:2023:949, para. 36.

whether processing for another purpose is compatible with the purpose for which the personal data are initially collected, take into account, inter alia:

(a) any link between the purposes for which the personal data have been collected and the purposes of the intended further processing;

(b) the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller;

(c) the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 10, or whether personal data related to criminal convictions and offences are processed, pursuant to Article 11;

(d) the possible consequences of the intended further processing for data subjects;

(e) the existence of appropriate safeguards, which may include encryption or pseudonymisation.

34. Article 9(1) and (2) of the Regulation provides that:

1. Without prejudice to Articles 4 to 6 and 10, personal data shall only be transmitted to recipients established in the Union other than Union institutions and bodies if:

(a) the recipient establishes that the data are necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the recipient; or

(b) the recipient establishes that it is necessary to have the data transmitted for a specific purpose in the public interest and the controller, where there is any reason to assume that the data subject's legitimate interests might be prejudiced, establishes that it is proportionate to transmit the personal data for that specific purpose after having demonstrably weighed the various competing interests.

2. Where the controller initiates the transmission under this Article, it shall demonstrate that the transmission of personal data is necessary for and proportionate to the purposes of the transmission by applying the criteria laid down in points (a) or (b) of paragraph 1.

35. Article 26(1) of the Regulation provides that:

The controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation.

36. Article 29(3)(a) of the Regulation requires a controller-processor agreement to set out "*the nature and purpose of the processing*" and "*the type of personal data*" and to provide that the processor *"[process] the personal data only on documented instructions from the controller*".

37. Article 29(10) of the Regulation provides that:

Without prejudice to Articles 65 and 66, if a processor infringes this Regulation by determining the purposes and means of processing, the processor shall be considered to be a controller in respect of that processing.

38. Article 30 of the Regulation provides that:

> *The processor and any person acting under the authority of the controller or of the processor, who has access to personal data, shall not process those data except on instructions from the controller, unless required to do so by Union or Member State law.*

3.1.2. Analysis

39. As noted in paragraph 26, the Commission's use of Microsoft 365 is based on the 2021 ILA and all processing by Microsoft on the Commission's behalf for providing its services is regulated by the DPA. The permitted purposes of processing under the 2021 ILA are fixed in three different sections of the DPA: the main body of the DPA (applicable to online services generally);[24] the Software DPA Terms (applicable to certain on-premise software);[25] and the terms applicable to professional services.[26] In each case, processing is permitted firstly, to "*provide*" the services and secondly, for the purposes of Microsoft's "*business operations*". What it means to "*provide*" the services is defined in similar terms in all three sections, but with adaptations to reflect the different nature of each service area. The concept of Microsoft's "*business operations*" is defined in the same way in each case.[27]

3.1.2.1. Types of personal data

40. As noted in paragraph 27, the various types of data processed under the DPA are defined and distinguished from each other using Microsoft's typology ("*Customer Data*", "*Diagnostic Data*", "*Service Generated Data*", "*Professional Services Data*", "*Support Data*", "*Functional Data*").[28] This distinguishes types of data by reference to the service context in which they are either provided to Microsoft or otherwise obtained or generated by it.

41. The DPA does not fix which types of personal data are processed in the different service contexts and therefore subject to the different sets of data protection terms it contains. The main body of the DPA, the "*Software DPA Terms*"[29] and the terms governing professional services[30] each contain a section on "*Processing Details*" that purports to describe the types of data that are subject to each set of terms respectively.[31]

---

[24] Sections on "*Nature of Data Processing; Ownership*", "*Processing to Provide Customer the Online Services*" and "*Processing for Microsoft's Business Operations*" in the main body of the DPA, 2021 ILA, pp. 28-29.

[25] Sections on "*Nature of Data Processing*", "*Processing to Provide Customer the Software*" and "*Processing for Microsoft's Business Operations*" in the Software DPA Terms, 2021 ILA, pp. 52-53.

[26] Sections on "*Processing of Professional Services Data; Ownership*", "*Processing to Provide Customer the Professional Services*" and "*Processing for Microsoft's Business Operations*" in Chapter 4 of Attachment 1 of the DPA, 2021 ILA, pp. 65-66. As defined in the 2021 ILA, p. 5: *"'Professional Services'" means Product support services and Microsoft consulting services provided to Customer under this agreement. 'Professional Services' does not include Online Services."*

[27] The 2021 ILA has been amended, also with regard to processing for business operations, which is analysed in more detail in section 3.1.2.3.

[28] DPA's definitions, 2021 ILA, pp. 25-26.

[29] Chapter 2 of Attachment 1 of the DPA.

[30] Chapter 4 of Attachment 1 of the DPA.

[31] 2021 ILA, pp. 31, 54, 66.

42. The descriptions of the types of data are circular, however. The types of data are stated to "*include*" personal data falling within certain defined terms in Microsoft's typology, yet these terms are themselves defined by reference to the type of service context.[32] The types of personal data processed within each service context are therefore defined by reference to those same service contexts.

43. In its reply to the preliminary assessment, the Commission considers that "*the categories of personal data processed by Microsoft under the ILA are divided in the DPA into three data types: Customer Data, Service Generated Data and Diagnostic Data*" and that "*these data types are in fact defined.*"[33] For the reasons set out below, the EDPS however maintains that certain types of personal data have not been specified as required by the Regulation and as explained below and in particular in paragraphs 55 to 61 and 63 of this decision.

44. As regards **service generated data**, the Commission's 2021 Data Protection Impact Assessment[34] (the '2021 DPIA') states that:

> "*Microsoft does NOT publish a schema or inventory of Service Generated Data as this is of a proprietary nature applicable to the unique design of Microsoft cloud computing. As well as protecting MS intellectual assets, disclosure of this schema is a security risk.*"[35]

The EDPS therefore considered in its preliminary assessment that it was not possible for the Commission or the EDPS to ascertain with any certainty which types of personal data fall within service generated data. The Commission had stated its understanding that service generated data were 'logs'.[36] The EDPS did not consider this explanation to shed further light on what personal data were processed in this context.

45. In its reply to the preliminary assessment, the Commission states that service generated data are processed when processing operations make use of online services.[37] According to the Commission, the nature of service generated data can be inferred from the description of service generated data under the 2021 ILA,[38] which states that:

> "*Service Generated Data means data generated or derived by Microsoft through the operation of an Online Service, and includes data generated in Microsoft's cloud infrastructure.*"[39]

---

[32] 2021 ILA, pp. 31, 54, 66. The main body of the DPA, p. 31 of the 2021 ILA, states that: "*The types of Personal Data processed by Microsoft when providing the Online Service include:*
(i) Personal Data that Customer elects to include in Customer Data (a template for the Customer to document the Categories of Data is provided for informational purposes in Attachment 5); and
(ii) those expressly identified in Article 3 of the EUDPR that may be contained in Diagnostic Data or Service Generated Data.
The types of Personal Data that Customer elects to include in Customer Data may be any categories of Personal Data, including the categories of Personal Data set forth in Attachment 5 of the DPA. Notwithstanding the foregoing, categories of data excludes operational personal data as defined in Article 3(2) of the EUDPR."

[33] Commission's reply of 25 May 2023, para. 111.

[34] Data Protection Impact Assessment report of October 2021 on the deployment of Microsoft's M365 services in the European Commission.

[35] Commission's 2021 DPIA, section 3.6.9, p. 42. Referenced again in the Commission's additional reply of 7 June 2022, p. 7.

[36] Minutes of the evidence-gathering meeting held on 28 November 2021, p. 12.

[37] Commission's reply of 25 May 2023, para. 23.

[38] Commission's reply of 25 May 2023, para. 23.

[39] 2021 ILA, pp. 26 and 50.

The EDPS considers that this contractual wording in essence only describes the general way in which service generated data are created and does not allow any discernment as to the actual types of personal data falling within the service generated data.

46. In its reply to the preliminary assessment, Microsoft Ireland has submitted excerpts of service generated data with pseudonymous identifiers.[40] The EDPS does not consider the excerpts to provide the information as to the types of personal data that are contained within the service generated data, as required by the Regulation.[41] This is because the excerpts represent a selected snapshot of the service generated data and do not allow understanding of the types of service generated data that are not contained in the excerpts.

47. The Commission further states that the assessment regarding the principle of purpose limitation allows for the overall documentation of the controller to be taken into account, not just the ILA.[42] This includes the DPIA, record of processing, privacy statements and products specific terms.[43] The record of processing which the Commission refers to states that:

> "*Service generated data (SGD) contains information related to the data subjects' usage of online services, most notably the user IP address, creation time, site URL and user email address. This data is generated by events that are related to user activity in Office 365. To learn which events trigger the creation of SGD, consult Annex A to the privacy statement.*"[44]

The corresponding privacy statement for Commission staff included in the record in addition states that:

> "*Event data will allow to monitor all activity in the cloud environment of each user.*"[45]

In its reply to the preliminary assessment, the Commission also states that:

> "*Microsoft confirms that [service generated data] capture events occurring in the cloud and can include customer (tenant) organisational identifiers, subscriptions, technical settings and resource names, configuration and device information, timestamps, URLs.*"[46]

The EDPS welcomes the inclusion of the four specific examples of service generated data in the record of processing activities.[47] However, those examples do not constitute a list specifying the types of personal data contained in service generated data as required by

---

[40] Reply by Microsoft Ireland of 26 May 2023, Annex 5, para. 102, Annex 4, p. 11, and PowerPoint presentation displayed at the hearing of 23 October 2023, p. 5.

[41] See paras. 55 to 61 and 63 of this decision.

[42] Commission's reply of 25 May 2023, para. 23.

[43] Commission's reply of 25 May 2023, para. 23.

[44] https://ec.europa.eu/dpo-register/detail/DPR-EC-04966.4, Section 3, para. 4. See similarly section 4 point 4 in "EC M365 environment privacy statement.pdf" and section 4 point 3 in "EC M365 environment guest user privacy statement.pdf" (both privacy statements included in the record under Section 7).

[45] Section 4, point 4 in "EC M365 environment privacy statement.pdf" included in the record, https://ec.europa.eu/dpo-register/detail/DPR-EC-04966.4, Section 7.

[46] Commission's reply of 25 May 2023, para. 57.

[47] https://ec.europa.eu/dpo-register/detail/DPR-EC-04966.4, Section 3, para. 4. See similarly section 4, point 4 in "EC M365 environment privacy statement.pdf" and section 4 point 3 in "EC M365 environment guest user privacy statement.pdf" (both privacy statements included in the record under Section 7).

the Regulation.[48] Nor do the examples of the types of data for which, according to the Commission, Microsoft confirms that they can be included in the service generated data[49] constitute such a list. In this regard, the EDPS stresses that it is not necessary to specify individual datasets, but rather the *types* of personal data processed. This would allow the Commission as the controller to ensure and be able to demonstrate compliance with the Regulation.

48. In its reply to the preliminary assessment, the Commission further states that:

> "*The definition brought forward in the contract provides a reasonable understanding of the personal data falling within [service generated data]. This is also evident by the fact that the Commission has been able to provide clear explanation in Annex A to the Privacy Statement. This document contains a list of [service generated data] that is logged through user activity in relation to each service used (e.g. for OneDrive for Business and SharePoint Online or Teams).*"[50]

The EDPS rejects that statement as inaccurate. Annex A to the privacy statement does not contain a list of service generated data but rather events that trigger the creation of service generated data. Such a list does not allow the reader to understand what types of personal data are processed within the scope of service generated data.

49. In its reply to the preliminary assessment, Microsoft Ireland refers to the following examples of types of logs containing service generated data that may be recorded: infrastructure and platform logs,[51] internal system events logs,[52] customer requests and server traffic logs[53] and customer event logs.[54] The EDPS considers that, apart from rare instances, these descriptions do not allow any discernment as to the actual types of personal data falling within the service generated data. In those rare instances, the descriptions only contain limited examples of concrete types of personal data within the service generated data.[55]

---

[48] See paras. 55 to 61 and 63 of this decision.

[49] Commission's reply of 25 May 2023, para. 57.

[50] Commission's reply of 25 May 2023, para. 56.

[51] According to Microsoft, these are logs to monitor, including in real time, the status of the different IT components that form part of the infrastructure of the cloud services provided by Microsoft, and communication between systems in different data centres are also logged. According to Microsoft, "*these logs do not contain customer personal data*" (reply by Microsoft Ireland of 26 May 2023, Annex 3, pp. 3 and 4).

[52] According to Microsoft, these logs record events that occur within internal service software, such as start or stop of service, client/server service transactions between components, configuration changes and software update events (reply by Microsoft Ireland of 26 May 2023, Annex 3, p. 4).

[53] According to Microsoft, these logs record exchanges of "client/server" traffic when Microsoft systems interact with customer systems, such as a user browser, client-side application, or Microsoft-provided software (reply by Microsoft Ireland of 26 May 2023, Annex 3, p. 4).

[54] According to Microsoft, these logs record events when customers initiate actions in enterprise cloud services, such as creating, reading, updating or deleting data or creating, committing or rolling back a database (reply by Microsoft Ireland of 26 May 2023, Annex 3, p. 4).

[55] According to Microsoft Ireland, some logs, e.g. in message tracing in Exchange Online, at the time of creation contain information, e.g. "user principal names", that directly identify the applicable users (reply by Microsoft Ireland of 26 May 2023, Annex 3, pp. 4 and 5, and Annex 6, p. 4). The EDPS understands that these logs may therefore contain also non-pseudonymous personal data. Microsoft Ireland also gave the example of a log showing the input of Teams Usage per tenant per user on various devices, operating systems and platforms, which among others, contains pseudonymous identifier fields such as "user ID" (reply by Microsoft Ireland of 26 May 2023, Annex 4, p. 11).

50. With regard to the types of data contained in service generated logs, Microsoft Ireland also states that:

> "*customer access to logs generated within Microsoft enterprise cloud service is enabled as part of the services to address* [...] *customer self-service logging features* [...] *and fulfilling data subject requests.*"[56]

Microsoft Ireland further states that:

> "[it] *provides extensive documentation to customers and would-be customers on logs and what types of data, personal or otherwise, would be contained in logs. While* ***not exhaustive****, this documentation supports customers' ability to assess the risk of processing of personal data outside of Customer Data when using Microsoft services*". (emphasis added)[57]

However, the EDPS does not consider that such access and documentation demonstrate that the Commission as the controller has defined the types of personal data contained within the service generated data as required by the Regulation.[58] Indeed, as acknowledged by Microsoft Ireland, the documentation is not exhaustive. The information that Microsoft Ireland has provided to the EDPS in relation to the access and documentation in question does not allow for specific types of personal data falling within service generated data contained in the logs to be identified either by the EDPS or the Commission. Therefore, it also does not allow the Commission to adequately assess the risks to data subjects.

51. Similarly, **diagnostic data** are also described in only a general way in the 2021 ILA and other documentation of the controller. The 2021 ILA provides that:

> "*Diagnostic Data means data collected or obtained by Microsoft from software that is locally installed by Customer in connection with the Online Service. Diagnostic Data may also be referred to as telemetry. Diagnostic Data does not include Customer Data or Professional Services Data.*"[59]

The record of processing, provided by the Commission in its reply to the preliminary assessment, states that:

> "*Diagnostic data (also known as telemetry data) is related to the data subjects' usage of office client software.*"[60]

The EDPS considers that these descriptions do not allow any discernment as to the actual types of personal data falling within the diagnostic data.

52. In its reply to the preliminary assessment, Microsoft Ireland illustrates the different types of data that are processed "*when an individual is working with the Microsoft Teams online communication and collaboration platform*".[61] Microsoft illustrates those types of data by

---

[56] Reply by Microsoft Ireland of 26 May 2023, Annex 3, p. 7.
[57] Reply by Microsoft Ireland of 26 May 2023, Annex 3, pp. 7 and 8.
[58] See paras. 55 to 61 and 63 of this decision.
[59] 2021 ILA, p. 25.
[60] https://ec.europa.eu/dpo-register/detail/DPR-EC-04966.4, Section 3, para. 3. See similar description of diagnostic data in section 4.3 in "EC M365 environment privacy statement.pdf" included in the record.
[61] Reply by Microsoft Ireland of 26 May 2023, Annex 6, pp. 1-2.

using similar definitions as "*per the Custom DPA with the EU institutions*" of customer data, diagnostic data, functional data, personal data, professional services data and service general data.[62]

Microsoft Ireland also states that:

> "*Through the Diagnostic Data Viewer, customers can view Office Diagnostic Data collected by the Teams client software. Customers can also access personal data, including that in Diagnostic Data, by using tooling to support data subject request (DSRs), which enables the customer organization to access and export the personal data Microsoft has retained from the user's (data subject's) interactions with online services. This includes pseudonymous personal data from Diagnostic Data collected by Microsoft.*"[63]

Microsoft also refers to documentation provided on its website for information on diagnostic data collection and controls.

The EDPS does not consider that such access and documentation demonstrate that the Commission, as the controller for the processing in its use of Microsoft 365, has specified the types of personal data contained within the diagnostic data as required by the Regulation.[64] The information that Microsoft Ireland has provided to the EDPS in relation to the access and documentation in question does not allow for specific types of personal data falling within diagnostic data to be identified either by the EDPS or the Commission.

53. The contractual wording also does not contribute to the delimitation of the scope of personal data falling within the service generated data and diagnostic data. According to 2021 ILA, data "*expressly identified in Article 3 [of the Regulation]*" may be contained in diagnostic data or service generated data, with the exception of operational personal data as defined in Article 2(3) of the Regulation.[65] It follows that the service generated data or diagnostic data may consist of any personal data, except operational personal data.

54. In the EDPS' view, it is not clear precisely what types of personal data are being collected and further processed in the context of service generated data and diagnostic data for the purposes set out in the DPA.

55. In accordance with Article 4(1)(b) of the Regulation, personal data must be collected for specified and explicit purposes. [66] It follows from the case-law of the Court of Justice of the EU (the 'Court of Justice') that the purposes of the processing are to be identified at the latest at the time of the collection of the personal data and that the purposes of that processing are to be clearly stated.[67] Also, such purposes are to guarantee, inter alia, the

---

62 Reply by Microsoft Ireland of 26 May 2023, Annex 6, pp. 1-2.

63 Reply by Microsoft Ireland of 26 May 2023, Annex 6, p. 2.

64 See paras. 55 to 61 and 63 of this decision.

65 2021 ILA, pp. 31 and 54. The EDPS notes that according to the 2021 ILA, Attachment 5 to the DPA, which contains completed checkboxes of personal data, covers personal data that the Commission elects to include in customer data, professional services data and functional data. It does not, however, cover personal data contained in service generated data or diagnostic data. (2021 ILA, pp. 31, 54 and 66).

66 See, to that effect, judgment in Case C-77/21, *Digi*, ECLI:EU:C:2022:805, para. 25, and judgment in Case C-175/20, *Valsts ieņēmumu dienests (Processing of personal data for tax purposes)*, EU:C:2022:124, para. 63.

67 See, to that effect, judgment in Case C-77/21, *Digi*, ECLI:EU:C:2022:805, para. 27, and judgment in Case C-

lawfulness of the processing of those data under Article 5(1) of the Regulation.[68] Under Article 4(2) of the Regulation, the controller is responsible for compliance with each of the principles of paragraph 1 of that Article and bears the burden of demonstrating such compliance.[69]

56. In Article 4(1)(b) of the Regulation, "*specified*" implies that the purpose of the collection must be clearly and specifically identified: it must be detailed enough to determine what kind of processing is and is not included within the specified purpose. Clarity in this regard is necessary for both the controller and the supervisory authority to determine whether each processing complies with the law and what data protection safeguards should be applied.[70]

57. Pursuant to Article 3(8) of the Regulation, it is for the EU institution or body as the controller to determine the purposes and the (essential) means of the processing. Such essential means include what personal data of which data subjects are processed by whom and for how long.[71] Essential means are means that are closely linked to the purpose and the scope of the processing. Together with the purpose of processing, the essential means are also closely linked to the question of whether the processing is lawful, necessary and proportionate.[72]

58. The EDPS considers that determining what kind of processing falls within the purpose limitation inherently implies identifying what types of personal data are to be processed. Indeed, without identifying what types of personal data are processed for what purposes, neither the controller nor the competent supervisory authority can assess whether the processing complies with the law.[73] This exercise is all the more important where the processing of special categories of personal data is not excluded, as it is not excluded under the 2021 ILA with regard to service generated data and diagnostic data.[74] This is

175/20, *Valsts ienemumu dienests (Processing of personal data for tax purposes)*, EU:C:2022:124, paras. 64 to 66. See also by analogy judgment in Case C-205/21, *Ministerstvo na vatreshnite raboti (Enregistrement de données biométriques et génétiques par la police)*, ECLI:EU:C:2023:49, paras 66 and 124.

[68] See, to that effect, judgment in Case C-77/21, *Digi*, ECLI:EU:C:2022:805, para. 27, and judgment in Case C-175/20, *Valsts ienemumu dienests (Processing of personal data for tax purposes)*, EU:C:2022:124, paras. 64 to 66. See also by analogy judgment in Case C-205/21, *Ministerstvo na vatreshnite raboti (Enregistrement de données biométriques et génétiques par la police)*, ECLI:EU:C:2023:49, paras 66 and 124.

[69] See, to that effect, judgment in Case C-60/22, *Bundesrepublik Deutschland*, ECLI:EU:C:2023:373, paras. 32 and 53, judgment in Case C-175/20, *Valsts ieņēmumu dienests (Processing of personal data for tax purposes)*, EU:C:2022:124, paras. 77, 78 and 81, and judgment in Case C-340/21, *Natsionalna agentsia za prihodite*, ECLI:EU:C:2023:986, paras. 49 to 52, 55 and 57, as well as the judgment in Case C-77/21, *Digi*, ECLI:EU:C:2022:805, para 24, and the Opinion of the Advocate General Pikamäe in that case (ECLI:EU:C:2022:248), point 47. See also EDPB Binding Decision 3/2022 on the dispute submitted by the Irish SA on Meta Platforms Ireland Limited and its Facebook service (Art. 65 GDPR), para. 105, EDPB Binding Decision 4/2022 on the dispute submitted by the Irish SA on Meta Platforms Ireland Limited and its Instagram service (Art. 65 GDPR), para. 108, and EDPB Binding Decision 5/2022 on the dispute submitted by the Irish SA regarding WhatsApp Ireland Limited (Art. 65 GDPR), para. 101.

[70] Article 29 Working Party Opinion 3/2013 on purpose limitation of 2 April 2013, p. 15. See also EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR, p. 35. As regards the importance of setting out sufficiently specified purpose of the processing see also the Opinion of Advocate General Pikamäe, C-77/21, *Digi*, ECLI:EU:C:2022:248, points 40 to 47, and judgment in the same case, ECLI:EU:C:2022:805, paras. 24 to 27 and 47 to 49.

[71] EDPS Guidelines on the concepts of controller, processor and joint controllership under Regulation (EU) 2018/1725, pp. 9-10 and 16-17.

[72] EDPB Guidelines 07/2020, para. 40.

[73] See in this respect also Opinion of the Advocate General Pitruzzella, Case C-817/19, *Ligue des droits humains*, ECLI:EU:C:2022:65, points 113, 130 and 131.

[74] 2021 ILA, p. 31. See also para. 72 of this decision.

because the processing of special categories of personal data is subject to more stringent data protection requirements under Article 10 of the Regulation.

59. The ultimate objective of the requirement that the purpose of the collection be "*explicit*" is to ensure that it is specified without vagueness or ambiguity as to its meaning or intent.[75] The purposes must, in particular, be expressed in a way that allows the controller, any third-party processors, supervisory authorities and data subjects to understand them in the same way.[76] They must be sufficiently clear to all involved, irrespective of their level of understanding.[77]

60. Any lack of clearly identified purposes and types of personal data also undermines the ability of the controller to comply with other principles, such as data minimisation which requires that the processing of personal data does not go beyond what is necessary for the specified purposes.[78]

61. The EDPS considers that where a purpose for collecting personal data is not clearly linked to specific types of personal data, that purpose has not been specified explicitly.[79] This shortcoming is not remedied by establishing a typology of data in which unspecified types of personal data are classified according to the business context in which they are processed.

62. It follows that the types of personal data collected and further processed under the 2021 ILA, and in particular service generated data and diagnostic data, have not been sufficiently determined in relation to each of the purposes of the processing so as to allow those purposes to be explicit and specified. This is in breach of Article 4(1)(b) of the Regulation.

63. The fact that the 2021 ILA or another legal act that is binding on the processor[80] insufficiently sets out the types of personal data to be processed also infringes Article 29(3) of the Regulation. As emphasised by the European Data Protection Board ('EDPB'), Article 28(3) GDPR (equivalent to Article 29(3) of the Regulation) requires that the contract or another legal act under EU or Member State law set out the type of personal data to be processed, specifying it in the most detailed manner possible (e.g. video images

---

75 Article 29 Working Party Opinion 3/2013, p. 17.
76 Article 29 Working Party Opinion 3/2013, p. 17.
77 Article 29 Working Party Opinion 3/2013, p. 17.
78 See, by analogy, EDPB Binding Decision 3/2022 on the dispute submitted by the Irish SA on Meta Platforms Ireland Limited and its Facebook service (Art. 65 GDPR), footnote 197, EDPB Binding Decision 4/2022 on the dispute submitted by the Irish SA on Meta Platforms Ireland Limited and its Instagram service (Art. 65 GDPR), footnote 184, and EDPB Binding Decision 5/2022 on the dispute submitted by the Irish SA regarding WhatsApp Ireland Limited (Art. 65 GDPR), footnote 142. In para. 109 of the EDPB Binding Decision 5/2022, the EDPB was, for example, of the opinion that "*WhatsApp IE is under the legal duty to assess whether the processing of all its users data is necessary for the purpose of service improvements or if there are alternative, less intrusive ways to pursue this purpose (e.g. instead of relying on all users' data for the purpose of service improvements, rely on a pool of users, who voluntarily agreed, by providing consent, to the processing of their personal data for this purpose)*". In para. 153 of that binding decision, the EDPB also, for example, considered that "*the processing by WhatsApp IE cannot be regarded as ethical and truthful* [and thus fair] *because it is confusing with regard to the type of data processed, the legal basis used and the purposes of the processing, which ultimately restricts the WhatsApp IE's users' possibility to exercise their data subjects' rights*".
79 See in this respect also the EDPB report on the 2022 Coordinated enforcement action on the use of cloud-based services by the public sector, 17 January 2023, in the report (p. 13, 15, 30 and 31) and annex (pp. 50, 51, 77, 79, 80, 102, 105, 106).
80 See para. 71 of this decision.

of individuals as they enter and leave a facility).[81] The EDPB considers that it is insufficient merely to specify that the processing concerns "*personal data pursuant to Article 4(1)[82] GDPR*" or "*special categories of personal data pursuant to Article 9[83] [GDPR]*".[84]

64. In its reply to the preliminary assessment, Microsoft Ireland states that:

> *"The EDPS' preliminary finding in para. 41 of its Preliminary Assessment, which concludes that the processing purposes and the data categories must be linked in order to satisfy the purpose limitation principle, is not based on any requirement in the EUDPR or the Art. 29 SCCs."*[85]

In response to that statement, the EDPS refers to paragraphs 56 to 60 of this decision. In order to comply with Article 4(1)(b) of the Regulation (and allow that provision to achieve its *effet utile*) a purpose for collecting personal data must be linked to specific types of personal data. Microsoft Ireland has not put forward specific arguments repudiating that reasoning, which was already provided in the preliminary assessment.

65. In its reply to the preliminary assessment, Microsoft Ireland also states that:

> "*There is no legal requirement nor explicit guidance from the EDPS or EDPB to adopt any specific level of granularity when describing data categories*".[86]

By referring to EDPB Opinion 14/2019 on the draft standard contractual clauses ('SCCs') submitted by the Danish supervisory authority,[87] Microsoft Ireland further states that:

> *"The EDPS [sic] itself has always interpreted Art. 29 EUDPR as requiring 'describing' the data categories that are processed rather than exhaustively set out each single one of them."*[88]

The EDPS rejects those statements as inaccurate. The EDPB held the same view in its Opinion 14/2019 referred to by Microsoft Ireland as in its Guidelines 07/2020 referred to in paragraph 63 of this decision. According to EDPB Opinion 14/2009, the description of the types of personal data and purposes of the processing should be made, in the contract or another legal act, "*in the most detailed possible manner, and, in any circumstance, the types of personal data must be specified further than merely 'personal data as defined in article 4(1)'*" GDPR.[89] Moreover, the purposes of the processing and types of personal data should be determined taking into account the specific tasks and responsibilities of the processor in the context of the processing to be carried out and the risk to the rights and freedoms of the data subjects.[90]

---

81 EDPB Guidelines 07/2020, para. 114.
82 Equivalent to Article 3(1) of the Regulation.
83 Equivalent to Article 10 of the Regulation.
84 EDPB Guidelines 07/2020, para. 114. See also Commission's reply of 25 May 2023, paras. 52 and 53.
85 Reply by Microsoft Ireland of 26 May 2023, para. 155.
86 Reply by Microsoft Ireland of 26 May 2023, para. 163.
87 EDPB Opinion 14/2019 on the draft Standard Contractual Clauses submitted by the DK SA (Article 28(8) GDPR), para. 50.
88 Reply by Microsoft Ireland of 26 May 2023, para. 163.
89 EDPB Opinion 14/2019, para. 50. See also EDPB Guidelines 07/2020, para. 114.
90 Recital 51 of the Regulation.

66. In this regard, Microsoft Ireland also states that:

> "*Art. 29 SCCs [...] which are considered to be the 'gold standard' for Art. 29 compliance, do not require the details of processing to be set out with any specific level of granularity. The Art. 29 SCCs simply require the controller and processor to specify the processing purposes and data categories in Annex II, using the level of detail* ***they consider appropriate.***" (emphasis added).[91]
>
> *"When comparing this against the position taken in Annex III of the Art. 29 SCCs (which sets out the description of the technical and organizational security measures), it becomes clear that more granularity is intended and needed in Annex III for the technical and organizational security measures. Annex III includes an 'explanatory note' which requires that 'the technical and organizational measures need to be described concretely and not in a generic manner'. Such an explanatory note was purposely not included in Annex II, which is an indication that this level of detail is not meant to be included in a description of the processing details.*" [92]

The EDPS rejects the interpretation of Article 29(3) of the Regulation put forward by Microsoft Ireland[93] which stems from Implementing Decision (EU) 2021/915 laying down the so-called Article 29 SCCs.[94] Annex II to that Implementing Decision indeed does not contain instructions as to the level of granularity of the categories of personal data processed. However, that does not imply that, as suggested by Microsoft Ireland, the controller and processor are free to specify the types of personal data as "*they consider appropriate*", for the following reasons.

67. First, only the controller is to set out the types of personal data processed, as it must determine the purposes and means of processing.

68. Second, in doing so, the controller must set out the types of personal data in compliance with other provisions of the Regulation, such as Article 4(1)(b). The controller must also be able to demonstrate that it has done so.[95] Such specification of the types of personal data may in any event be subject to an assessment by the EDPS as a supervisory authority tasked with monitoring and ensuring compliance with the Regulation. Also, such specification may be further subject to judicial review.[96] It cannot be, as suggested by Microsoft Ireland, left to the unrestrained discretion of the controller and processor. The EDPS stresses that its interpretation of the requirements of the Regulation as to the

---

[91] Reply by Microsoft Ireland of 26 May 2023, para. 152. In footnote 74 to the same para., Microsoft Ireland also states that Annex II goes on to leave discretion to the contractual parties to include a description "*they see fit*".

[92] Reply by Microsoft Ireland of 26 May 2023, para. 153.

[93] Reply by Microsoft Ireland of 26 May 2023, para. 152.

[94] Commission Implementing Decision (EU) 2021/915 of 4 June 2021 on standard contractual clauses between controllers and processors under Article 28(7) of Regulation (EU) 2016/679 of the European Parliament and of the Council and Article 29(7) of Regulation (EU) 2018/1725 of the European Parliament and of the Council (OJ L 199, 7.6.2021).

[95] See, to that effect, judgment in Case C-60/22, *Bundesrepublik Deutschland*, ECLI:EU:C:2023:373, paras. 32, 53, and judgment in Case C-175/20, *Valsts ieņēmumu dienests (Processing of personal data for tax purposes)*, EU:C:2022:124, paras. 77, 78 and 81, as well as the judgment in Case C-77/21, *Digi*, ECLI:EU:C:2022:805, para 24.

[96] See, to that effect, the Opinion of the Advocate General Pikamäe in Case C-77/21, *Digi*, ECLI:EU:C:2022:248, point 47, and, by analogy, judgment in Case C-61/19, *Orange Romania*, EU:C:2020:901, paras. 51 and 52.

level of granularity of the types of personal data are consistent with EDPB Guidelines 07/2020 (see paragraphs 63 and 65 of this decision).

69. Third, Annex III to Implementing Decision (EU) 2021/915, as opposed to Annex II, indeed contains an explanatory note providing that technical and organisational measures need to be described concretely and not in a generic manner. However, that cannot be interpreted *a contrario* as absolving the controller from the requirements of the Regulation as to the level of granularity of the types of personal data to be set out in a contract or another legal act. The objective of the Implementing Decision (EU) 2021/915 is not to exhaustively reproduce all requirements of the Regulation or provide interpretations of its provisions.[97]

70. Microsoft Ireland further states that:

> "*The EDPS seems to rely unduly on certain general principles in the EUDPR, such as the accountability principle [...] and the purpose limitation principle [...] to support its preliminary assessment that the 2021 ILA is not sufficiently detailed to comply with the EUDPR. Whilst the general principles of processing are relevant, they remain high-level principles. Neither the EUDPR nor regulatory guidance from the EDPB or EDPS require or even link these general principles to the contractual language requirements under Art. 29 EUDPR. The only article in the EUDPR that applies directly to determine what must be included in a data processing agreement, is Art. 29 EUDPR (which, as set out above, does not impose this level of granularity).*"[98]

The EDPS rejects that statement. The general principles laid down in Article 4 of the Regulation relate to all processing of personal data and underpin all other provisions of the Regulation. The specific practical requirements stemming from the general principles are concretised in obligations set out in other provisions of the Regulation.[99] The general principles must be fully complied with in relation to all processing activities[100] and are to be used, in particular, when interpreting other provisions that regulate the same subject matter.[101] This certainly applies to the relationship between Article 4(1)(b) and Article 29(3) of the Regulation since both provisions aim to ensure that the purposes of the processing are appropriately specified.

---

[97] The contract between the EU institution as the controller and its service provider as the processor pursuant to Article 29 of the Regulation must reflect all the requirements of the Regulation, including imposing on the processor all corresponding obligations to ensure that the processing meets those requirements. As recognised in recital 66 of the Regulation and in recital 6 of Implementing Decision (EU) 2021/915, controllers and processor are encouraged to provide additional safeguards via contractual commitments that supplement standard contractual clauses.

[98] Reply by Microsoft Ireland of 26 May 2023, p. 48, footnote 90.

[99] See, to that effect, EDPB Binding decision 1/2021 on the dispute arisen on the draft decision of the Irish Supervisory Authority regarding WhatsApp Ireland under Article 65(1)(a) GDPR, paras. 188 to 192, where the EDPB analysed the relationship between the principle of transparency under Article 5(1)(a) of the GDPR and the obligations under Articles 12, 13 and 14 GDPR. The EDPB underlined that: "*the principle of transparency is not circumscribed by the obligations under Articles 12-14 GDPR, although the latter are a concretisation of the former*", "*the GDPR distinguishes the broader dimension of the principle from the more specific obligations*" and "*the transparency obligations do not define the full scope of the transparency principle*".

[100] See, to that effect, Case C-61/19, *Orange Romania*, points 32, 49 and 65 of the Opinion of Advocate General Szpunar, (ECLI:EU:C:2020:158), and para. 42 of the judgment (ECLI:EU:C:2020:901).

[101] See, to that effect, judgment in Case C-60/22, *Bundesrepublik Deutschland*, ECLI:EU:C:2023:373, paras. 52-58.

71. Even if the overall documentation is to be taken into account to assess compliance with Article 4(1)(b) of the Regulation, as stated by the Commission,[102] the controller must ensure compliance with Article 29(3) of the Regulation by way of a contract or another binding legal act. As a matter of principle, the objective of a record of processing activities and of a privacy statement containing information for data subjects is not to bind the processor as to the purposes and essential means of the processing. Instead, their objective is to provide basic and concise description of the processing so that the individuals concerned by the processing can be informed of the existence of the processing operation and its purposes. The record of processing activities also serves to help demonstrate compliance with the Regulation. However, it cannot demonstrate compliance with e.g. Article 29 of the Regulation where the necessary elements are not sufficiently set out in a contract or another binding legal act under Union or Member State law. The Commission and Microsoft Ireland have not demonstrated that the 2021 DPIA, record of processing activities, privacy statement or any other documents provided in their submissions are binding on Microsoft Ireland as the processor.[103]

72. It follows that the specification under the 2021 ILA that data "*expressly identified in Article 3 [of the Regulation]*" may be contained in diagnostic data or service generated data, with the exception of operational personal data as defined in Article 2(3) of the Regulation,[104] is in breach of Article 29(3) of the Regulation. In addition, the EDPS considers, in view of the above,[105] that even if the Commission had contractually made some or all of the overall documentation referred to in paragraph 71 of this decision binding on the processor, the types of personal data, and in particular service generated data and diagnostic data, would not have been set out as required by Article 29(3) of the Regulation.

73. As an ancillary note, the EDPS observes that German data protection authorities have reached similar conclusions in their assessment of Microsoft 365 on how types of personal data are insufficiently set out in the September 2022 Data Processing Agreement.[106] Other data protection authorities, such as the Greek and Lithuanian, have identified similar issues.[107]

74. In its reply to the preliminary assessment, Microsoft Ireland states that:

> "*The EDPB, in regulatory guidance, at various occasions recommends the use of a 'layered approach' for data protection compliance purposes – even in the context of a transparency notice, when the use of clear and comprehensive language is even more relevant.*[108] *This is exactly what Microsoft is doing by making available more detailed information online (e.g. through its online terms) for those who require more*

---

[102] Commission's reply of 25 May 2023, para. 23. See also para. 47 of this decision.
[103] See also para. 95 of this decision.
[104] 2021 ILA, p. 31.
[105] In particular paras. 49 to 53 of this decision.
[106] See the findings of the Conference of German DPAs on Microsoft Online Services (Microsoft 365), 24 November 2022, in summary (pp. 3 and 4) and assessment (pp. 7 to 11 and 13 to 15). See similarly the findings of the Baden-Württemberg DPA's audit of Microsoft 365 in the context of a pilot project on its possible use in schools (23 April 2021, published 25 April 2022), in particular in the Baden-Württemberg DPA's opinion (p. 8, 10 and 11).
[107] See in this respect the EDPB report on the 2022 Coordinated enforcement action on the use of cloud-based services by the public sector, 17 January 2023, in particular findings by the Greek and Lithuanian DPAs in annex (pp. 50, 51, 53, 95 and 96).
[108] Reply by Microsoft Ireland of 26 May 2023, para. 169.

detailed information. And this is also the approach the EDPS adopts in its website privacy notice."[109]

The EDPS rejects these statements as not applicable with regard to compliance with Article 4(1)(b) of the Regulation, in so far as it pertains to the determination of the types of personal data by the controller,[110] and Article 29(3) of the Regulation. Indeed, the EDPB and the EDPS recommend using a layered approach, however not "*even in the context of a transparency notice*" as stated by Microsoft Ireland, but rather solely in that context. The reason for this is not to overburden the average data subject but allow them to be immediately familiarised with the main elements related to the processing and to obtain further information on request. However, such a layered approach cannot apply to the (contractual) relationship between the controller and processor, where the types of personal data and purposes of the processing must be specified and set out in a binding legal act. This applies even more so since the Commission is a controller under the Regulation that carries out tasks in the public interest and is responsible for the processing of personal data of tens of thousands of data subjects.[111]

75. According to the Commission, Microsoft has invoked its right to (intellectual) property as a reason for not specifying the types of personal data falling within the concept of service generated data.[112] The Commission has stated that Microsoft contends that an exhaustive disclosure of such information would provide insights as to how Microsoft's processes work, allowing competitors to potentially re-create Microsoft's technology.[113] The Commission has also indicated that the disclosure of that information would constitute a security risk[114] and that, according to Microsoft, it would allow malicious actors to exploit this information to conduct malicious activities.[115]

76. According to the Commission, this does not permit the parties to the contract to comprehensively establish a definitive list of types of personal data with regard to service generated data.[116]

77. On the other hand, Microsoft Ireland states that:

"*Service-Generated Data is not data that is provided by any individual – it is automatically generated in the processing of System-Generated Logs by Microsoft. Therefore, it is* ***not possible for Microsoft to set out [service generated] data*** *categories* ***in detail in an exhaustive manner*** *(i.e. beyond what is currently set*

[109] Reply by Microsoft Ireland of 26 May 2023, para. 170, see also para. 168.
[110] As opposed to compliance with the obligation pursuant to Articles 14, 15 and 16 of the Regulation to provide relevant information to data subjects.
[111] Affected data subjects include not only all Commission's staff, but also staff of other EU institutions or bodies and other individuals, which e.g. cooperate with the Commission using the Commission's tools based on Microsoft 365 or whose personal data are otherwise processed when the Commission carries out its tasks using Microsoft 365.
[112] Commission's 2021 DPIA, section 3.6.9, p. 42. Referenced again in the Commission's additional reply of 7 June 2022, p. 7.
[113] Commission's reply of 25 May 2023, para. 55.
[114] Commission's 2021 DPIA, section 3.6.9, p. 42. Referenced again in the Commission's additional reply of 7 June 2022, p. 7.
[115] Commission's reply of 25 May 2023, para. 55. See also reply by Microsoft Ireland of 26 May 2023, Annex 3, p. 2, last para.
[116] Commission's 2021 DPIA, section 3.6.9, p. 42. Referenced again in the Commission's additional reply of 7 June 2022, p. 7. See also the Commission's reply of 25 May 2023, para. 55.

out in Attachment 5 of the 2021 ILA or our documentation on personal data in System-Generated Logs)" (emphasis added).[117]

The EDPS understands this statement as suggesting that the Commission cannot obtain sufficiently specified information as to the types of service generated data because it is not feasible for Microsoft to provide such information. This is different from invoking harm to Microsoft's commercial interests or a security risk. Moreover, this statement suggests that in particular the controller (the Commission), but also the processor (Microsoft Ireland) are not fully aware of the types of service generated data processed under 2021 ILA. This additionally substantiates the infringements of Articles 4(1)(b) and 29(3) of the Regulation as set out above. Those infringements are all the more serious given that logs contained in the service generated data continuously and automatically record[118] a large number of user activity events.[119] The EDPS therefore considers that such logging may enable tracking the activity of data subjects that are using Microsoft 365 in extreme detail. This is supported by the Commission's privacy statement which states that: "*Event data will allow to monitor all activity in the cloud environment of each user.*"[120] The logs contained in service generated data relate to the activities of individual users which can be identified, directly or indirectly.[121] Microsoft states that the focus is on system events, not individuals,[122] however that does not affect the fact that such logs relate to individual users. Given the stated risks to the rights of data subjects, sufficient clarity as regards the types of personal data concerned by both the controller and processor is therefore of utmost importance.

78. In principle, where a processor does not allow a controller to meet its obligations under the Regulation, the controller should ensure, pursuant to Articles 26(1) and 29(1) of the Regulation, that the corresponding processing does not take place. However, where another fundamental right (or a separate legal obligation) prevents the processor, and thereby the controller, from complying with the Regulation, the controller should, at the very least, satisfy itself that the resulting limitation respects the principle of proportionality before allowing such processing to start or continue.[123] The controller must be able to demonstrate that the processing complies with the Regulation.[124] This

[117] Reply by Microsoft Ireland of 26 May 2023, para. 172.
[118] Reply by Microsoft Ireland of 26 May 2023, Annex 3, p. 2.
[119] Commission's reply of 25 May 2023, Annex 2. This document shows hundreds of events of user activities that result in logs containing personal data, such as accessing, copying, deleting, modifying, previewing, uploading, downloading, renaming or moving a file, moving, accessing, deleting, sending or updating an email message, creating, modifying or updating inbox rules, starting and ending calls, including listing distinct identities involved in a call or associated with an online meeting etc.
[120] Section 4, point 4 in "EC M365 environment privacy statement.pdf" included in the record, https://ec.europa.eu/dpo-register/detail/DPR-EC-04966.4, Section 7.
[121] See paras. 163 to 170 of this decision.
[122] Reply by Microsoft Ireland of 26 May 2023, Annex 3, p. 2. See also Commission's reply of 25 May 2023, para 57, where the Commission states that: "*Microsoft confirms that SGD capture events occurring in the cloud and can include customer (tenant) organisational identifiers, subscriptions, technical settings and resource names, configuration and device information, timestamps, URLs*".
[123] Cf. Article 52(1) of the Charter of the Fundamental Rights of the EU.
[124] See, to that effect, judgment in Case C-60/22, *Bundesrepublik Deutschland*, ECLI:EU:C:2023:373, paras. 32, 53, judgment in Case C-175/20, *Valsts ieņēmumu dienests (Processing of personal data for tax purposes)*, EU:C:2022:124, paras. 77, 78 and 81, and judgment in Case C-340/21, *Natsionalna agentsia za prihodite*, ECLI:EU:C:2023:986, paras. 49 to 52, 55 and 57, as well as the judgment in Case C-77/21, *Digi*, ECLI:EU:C:2022:805, para 24, and the Opinion of the Advocate General Pikamäe in that case (ECLI:EU:C:2022:248), point 47.

includes demonstrating why any interference with the right to the protection of personal data is necessary and proportionate.

79. As a first step, and as part of the necessity test, it must be ensured that the selected measure is effective in achieving its objective and is the least intrusive.[125] When applying the necessity test, it should be borne in mind that derogations and limitations in relation to the protection of personal data must apply only in so far as is strictly necessary.[126] In this case, the Commission should have assessed, with the assistance of its processor as appropriate, whether any other less intrusive measure could be used by Microsoft Ireland to ensure the respect for the right of intellectual property and to adequately prevent security risks. In the preliminary assessment, the EDPS noted that in this context, the Commission should have obtained an explanation, by way of example, as to why a non-disclosure agreement between the Commission and Microsoft could not have adequately protected Microsoft's commercial interests. In this regard, the Commission's position as a major public institution should be taken into account in terms of reliability and confidentiality of any commitments that it would make in such an agreement.

80. The Commission has not provided the EDPS with any such assessment or explanation, nor has it demonstrated that it has sought to obtain such an explanation from Microsoft Ireland. The EDPS therefore considers that the necessity of the measure, i.e. limiting the specification of the types of service generated data, has not been established. When a measure, and the ensuing interference with the right to protection of personal data, are not established as being strictly necessary, it is no longer necessary to carry out a strict proportionality test.[127] This is because necessity is a pre-condition for proportionality.

81. Even if necessity had been established, the Commission has also not demonstrated[128] how the principle of strict proportionality has been respected with regard to the specification of the types of personal data contained in service generated data. It should have carried out a careful assessment, balancing the right to the protection of personal data against the right to property.[129] The EDPS has seen no evidence that the Commission has made such an assessment.

82. Nonetheless, the EDPS has carried out its own assessment as to whether the principle of strict proportionality has been respected, notwithstanding that the EDPS considers that already the principle of necessity has not been satisfied.

83. In their replies to the preliminary assessment, the Commission and Microsoft Ireland have provided additional information on the types of personal data contained in service

---

[125] See e.g. judgment in Case C-252/21, *Meta Platforms and Others (Conditions générales d'utilisation d'un réseau social)*, ECLI:EU:C:2023:537, paras. 97 to 126; judgment in Case C-184/20, *Vyriausioji tarnybinės etikos komisija*, ECLI:EU:C:2022:601, paras 85 and 96 to 99, 101 to 106, 110 to 113; judgment in Case C-439/19, *Latvijas Republikas Saeima (Penalty points)*, EU:C:2021:504, paras 98, 102 to 106 and 108 to 122; judgment in Case C-205/21, *Ministerstvo na vatreshnite raboti (Enregistrement de données biométriques et génétiques par la police)*, ECLI:EU:C:2023:49, paras. 114, 126 and 127. See also EDPS' toolkit for assessing the necessity of measures that limit the fundamental right to the protection of personal data. pp. 16 to 18.

[126] Judgment in Case C-13/16, *Rīgas satiksme*, ECLI:EU:C:2017:43, para. 30 and cited case-law; judgment in Case C-212/13, *Ryneš*, ECLI:EU:C:2014:2428, para. 28; judgment in Case C-708/18, *Asociaţia de Proprietari bloc M5A-ScaraA*, ECLI:EU:C:2019:1064, para. 46.

[127] Cf. Joined Cases C-465/00, C-138/01 and C-139/01, *Österreichischer Rundfunk and Others*, ECLI:EU:C:2003:294, paras. 90 to 92, as well as *Schrems*, C-362/14, ECLI:EU:C:2015:650, paras. 92 to 98. In Schrems I, the Court of Justice analysed the necessity and found the Safe Harbour Decision to be invalid, without making any reference to proportionality before reaching that conclusion.

[128] In its reply to the preliminary assessment or prior to that.

[129] Cf. *Promusicae*, C-275/06, ECLI:EU:C:2008:54, paras. 68 and 70. See also recital 4 of the GDPR.

generated data (see, in particular, paragraphs 45 to 49 of this decision). However, that information does not satisfy the requirements of Articles 4(1)(b) and 29(3) of the Regulation, as established above. The EDPS has carefully examined whether that additional information would adequately mitigate the interference with the right to the protection of personal data and the risks emanating from such interference. In particular, whether the mitigation of the interference would be such that the failure to specify the types of personal data as required by the Regulation could be deemed proportional to the protection of intellectual property and preventing of security risks in question.

84. First, it follows from the documents provided by the Commission and Microsoft Ireland that only a small share of the types of personal data falling within the scope of service generated data have been disclosed to the Commission and to the EDPS. Most types of personal data are therefore not specified or set out in a contract or another legal act binding on the processor. Second, as explained in paragraph 77, the EDPS considers that in the context of processing of service generated data, the risks to data subjects are particularly high, since the processing allows their activity to be tracked in extreme detail. In order to satisfy the principle of proportionality, the Commission would need to ensure that the interference with the rights of data subjects is mitigated. The mitigation in question might be achieved by contractually and actually limiting the extent of processing of service generated data. However, in order for the Commission to be in a position to limit the extent of processing of service generated data, the Commission would still have to be aware and in control as to what types of personal data are being or may be processed for what specific purposes in the Commission's use of Microsoft 365 and what events would cause such processing.

85. The EDPS therefore considers that the omission of the required specification of personal data contained in service generated data would not have been a proportionate measure to safeguard intellectual property or prevent security risks, even if the necessity of that measure had been established.

3.1.2.2. Processing for the provision of services

86. The 2021 ILA defines providing an online and professional service as follows:

"*Processing to Provide Customer the Online Services*
For purposes of this DPA, "to provide" an Online Service consists of:

- *Delivering functional capabilities as licensed, configured, and used by Customer and its users, including providing personalized user experiences and processing data as necessary to fulfil contractual obligations to Customer or to otherwise comply with law;*
- *Troubleshooting (preventing, detecting, and repairing problems affecting the operation of Online Services); and*
- *Ongoing improvement (installing the latest updates and capabilities, and making improvement to user productivity, reliability, efficacy, and security).*

When providing Online Services, Microsoft will not use or otherwise process Customer Data or Personal Data for: (a) user profiling, (b) advertising or similar commercial purposes, or (c) market research aimed at creating new functionalities, services, or products or any other purpose, unless such use or processing is in accordance with Customer's documented instructions.
For Online Services, which offer user profiling as part of the functionalities and features,

this will be described in the applicable documentation for the Online Service."[130]

"Processing to Provide Customer the Professional Services
For purposes of this Chapter 4, "to provide" Professional Services consists of:

- *Delivering the Professional Services, including providing technical support, professional planning, advice, guidance, data migration, deployment, and solution/software development services, and processing data as necessary to fulfill contractual obligations to Customer or to otherwise comply with law;*
- *Troubleshooting (preventing, detecting, investigating, mitigating, and repairing problems, including Security Incidents, affecting Customer's Professional Services); and*
- *Ongoing improvement (maintaining the Professional Services, including installing the latest updates and capabilities, and making improvements to the reliability, efficacy, quality, and security of the Professional Services).*

When providing Professional Services, Microsoft will not use or otherwise process Professional Services Data for: (a) user profiling, or (b) advertising or (c) market research aimed at creating new functionalities, services, or products or any other purpose or similar commercial purposes, unless such use or processing is in accordance with Customer's documented instructions."[131]

87. The EDPS has examined whether the Commission has complied with the Regulation with regard to the specification of the purpose of providing an online and professional service.[132] In that examination, the EDPS has focused on the following three issues.

88. **First**, in the preliminary assessment, the EDPS considered that the definitions of the provision of an online and professional service[133] were broad enough to include data analytics.[134] As a result, the EDPS was of the view that it was unclear whether processing for purposes such as training machine learning or artificial intelligence was permitted.

89. In its reply to the preliminary assessment, Microsoft Ireland states that:

> *"While [data analytics is] not a separate 'purpose' of processing in Microsoft 365, it is a computing mechanism that could be used to support the purposes described in the CTM DPA and is subject to all technical and organizational measures specified in the CTM DPA."*[135]
>
> *"More advanced features that could be characterized as providing a personalized service include Editor text predictions in Outlook or Word, where based on user typing the services use AI to predict and offer suggested text to the user."*[136]

The EDPS understands the first statement as acknowledging that the provision of an online and professional service may include data analytics. With regard to the second statement, the Commission has confirmed that it has enabled processor connected

[130] 2021 ILA, pp. 28 and 29.
[131] 2021 ILA, p. 65.
[132] 2021 ILA, pp. 28, 29 and 65.
[133] 2021 ILA, pp. 28, 29 and 65.
[134] Data analytics is the collection, transformation and organisation of data in order to draw conclusions, make predictions and drive informed decision-making.
[135] Reply by Microsoft Ireland of 26 May 2023, Annex 5, para. 70, fifth subpara.
[136] Reply by Microsoft Ireland of 26 May 2023, Annex 5, para. 71, third subpara.

experiences, including Editor which uses artificial intelligence.[137] It follows that Microsoft is using artificial intelligence in the context of providing online services to the Commission, without however specifying this in the 2021 ILA or another binding act under Article 29(3) of the Regulation. The use of artificial intelligence, while potentially improving the service provided, inherently poses potentially high risks to data subjects. Depending on the circumstances regarding its specific application and use, artificial intelligence may generate (high) risks and cause harm, material or immaterial, to public interests and rights that are protected by Union law.[138] The use of data analytics may also pose potentially high risks to data subjects, in particular where it is based on combining extensive datasets covering individuals' use of Microsoft 365 over a significant amount of time. The EDPS therefore considers that where the processing involves artificial intelligence or data analytics, the purposes of the processing must specify that in order for them to be considered specified and explicit. The Commission has failed to do that, and in particular in a contract or another binding legal act, in breach of Articles 4(1)(b) and 29(3) of the Regulation.

90. **Second**, "*ongoing improvement*" of a service is described as including "*making improvements to user productivity*",[139] to "*quality*"[140] and to "*efficacy*"[141] of the services concerned. It is unclear what productivity, quality and efficacy comprise. As noted in the preliminary assessment, it is not clear from the wording of the 2021 ILA whether improving user productivity comprises, for example, offering additional analytical services to the employer, analysing how much time employees spend in meetings or working on documents, or improving graphical interfaces by including additional shortcuts. It is not clear whether efficacy refers to energy efficacy (for example by modifying the code in order to shorten the computation time) or another type of efficacy.

91. In its reply to the preliminary assessment, the Commission states that:

> *"The Commission determined that the words 'making improvement to user productivity' and 'efficacy' sufficiently circumscribe the purposes of processing to which those words refer to. The description of the purposes and activities which the Commission instructs Microsoft to carry out in the context of a contract necessarily need to accommodate a certain degree of generalization to account for the complex service 'acquired' by the Commission via an interinstitutional contract. Even leaving aside for a moment the interinstitutional character of the contract, a healthy degree of general description of the purposes of processing is inherent in the flexibility needed for the contract to remain useful for the Commission as a modern and digitalised public administration. The design of any contract, including the definition of the purposes of processing, must be sufficiently flexible to usefully regulate the relationship between the parties, despite the de facto impossibility of any human being to list exhaustively all possible factual evolutions to which a contract might apply. The Commission has control and knowledge about what these activities entail*

[137] Commission's reply of 25 May 2023, para. 31, and 2021 DPIA. point 3.7.4.
[138] See the Commission Proposal for a regulation laying down harmonised rules on artificial intelligence, in particular recitals 4, 11, 18, 30, 33.
[139] Section on "*Processing to Provide Customer the Online Services*" in the main body of the DPA, 2021 ILA, p. 29.
[140] Section on "*Processing to Provide Customer the Professional Services*", Chapter 4, 2021 ILA, p. 65.
[141] Section on "*Processing to Provide Customer the Online Services*" in the main body of the DPA, 2021 ILA, p. 29, and section on "*Processing to Provide Customer the Professional Services*", Chapter 4, 2021 ILA, p. 65.

as these are addressed in section 3.10.2 of the DPIA (data types linked to a business process).”[142]

“For the avoidance of doubt, the Commission explains that ‘making improvement to user productivity’, ‘quality’ and ‘efficacy’ are to be understood as processing of personal data to make services more secure, more effective at achieving computing outcomes the service is intended to achieve (e.g. more effective screening of malware), more efficient in using computing resources to reduce service latency and to improve user interfaces always in relation to services to which customer subscribes.”[143]

The Commission has also cited a letter[144] in which Microsoft states that:

“[…] with respect to the expressions ‘making improvement to user productivity’ and to user ‘efficacy’, please note that these refer to the general notion that these expressions depict.”

The EDPS does not consider that those statements demonstrate compliance with Articles 4(1)(b) and 29(3) of the Regulation, for the following reasons.

92. The Regulation does not require that the Commission “*list exhaustively all possible factual evolutions to which a contract might apply*”.[145] In principle, no contract can provide exhaustively for all factual situations that may occur in the context of its implementation.[146] However, the purposes of the processing must be specified and explicit as required by Article 4(1)(b) of the Regulation and as explained in paragraphs 56 and 59 of this decision. The controller must set out such purposes in a contract or another binding legal act under EU or Member State law pursuant to Article 29(3) of the Regulation. A reference to the general meaning of the words “*making improvements to user productivity*” and “*efficacy*” does not sufficiently circumscribe the purposes to which those words refer. This view is analogous to the Article 29 Working Party Opinion 3/2013 according to which the purpose of “*improving users’ experience*” is considered too vague or general to meet the criterion of being specific, unless further details are provided.[147] Similarly, the EDPB has found that an average user cannot fully grasp what is meant by processing for service improvement where a company’s contract lacks clarity.[148] “*IT-security purposes*” are also considered in the Article 29 Working Party Opinion 3/2013 as too vague or general.[149] On a similar note, the EDPB has also noted that “*safety and security*” purpose is vague and highlighted “*that when the purpose of the processing is ‘IT*

[142] Commission’s reply of 25 May 2023, para. 39.
[143] Commission’s reply of 25 May 2023, para. 40.
[144] Commission’s substantive reply of 15 October 2021, paras. 2.3.1.5 and 2.3.1.6, p. 7.
[145] See para. 91 of this decision.
[146] As part of the controller’s instructions to its processor when any clarifications or changes to the processing are required once the processing operation has started, the contract must however set out the following. First, a procedure for how the contract is to be amended to clarify, amend or extend the scope of the processing, types of personal data or the purposes set out in the contract; and second, a procedure for how the controller is to supplement its instructions on how the processor is to process personal data on its behalf.
[147] Article 29 Working Party Opinion 3/2013, p. 16. The opinion further lists the following purposes as too vague or general: “*marketing purposes*” and “*future research*”.
[148] EDPB Binding Decision 5/2022 on the dispute submitted by the Irish SA regarding WhatsApp Ireland Limited (Art. 65 GDPR), paras. 111 and 114.
[149] Article 29 Working Party Opinion 3/2013, p. 16.

Security', for instance in the meaning of Article 32 GDPR, the purpose of the processing has to be clearly and specifically identified by the controller".[150]

93. Moreover, the Commission's explanations provided in its reply to the preliminary assessment as to how *"making improvement to user productivity", "quality" and "efficacy"* are to be understood, are not binding on the processor as required by Article 29(3) of the Regulation. The controller (or the processor) cannot remedy any non-compliance related to setting out elements in a contract or another binding legal act by listing such elements in a submission to the supervisory authority. Such a submission does, however, suggest that it is possible to further specify the purpose of the processing without losing the flexibility that needs to be maintained in a contractual relationship. The objective of setting out the purposes of the processing in an act that is binding on the processor is not only for the controller to clearly specify those purposes but mainly to ensure that the processor is bound by that specification. Failing that, the controller allows the processor to partially determine the purposes itself, in breach of the Regulation.

94. In its reply to the preliminary assessment, Microsoft Ireland states that in addition to any documents binding on Microsoft, the EDPS should in its assessment take into account:

> "*[...] any other documents which serve to clarify the processing details or instructions between the parties [...].*[151]
>
> *For example, under applicable contract law, the protection obtained by the Commission under the ILA can also include how the parties have been interpreting and executing the agreement. This includes certain explanations (and proposals) issued to the Commission by Microsoft, as well as the origins of the contractual relationship.*"[152]

In its reply, Microsoft Ireland also provides information on the purposes of the processing of different types of data, in particular service generated data, logs and diagnostic data.[153] Such purposes include keeping service secure and up-to-date, remediating problems and making product improvements.[154] The EDPS understands this information, which was provided after the reference date, as an example of explanations issued by Microsoft as referred to in the quoted statement.[155] In addition, Microsoft Ireland states that the applicable law is Belgian contract law.[156] However, according to 2021 ILA, applicable law governing it is EU law, complemented, where necessary, by the law of Belgium.[157]

95. In view of primacy of EU law, the Regulation and the contractual stipulation as to the applicable law governing the 2021 ILA, any national rule may only be applied in so far as it fully observes Article 29(3) of the Regulation. This means that Article 29(3) of the Regulation precludes any such rule that would fail to ensure that the purposes of the processing are set out in a contract or other legal act under EU or Member State law

[150] EDPB Binding Decision 5/2022 on the dispute submitted by the Irish SA regarding WhatsApp Ireland Limited (Art. 65 GDPR), paras. 90, 111 and 116.
[151] Reply by Microsoft Ireland of 26 May 2023, Annex 5, para. 13.
[152] Reply by Microsoft Ireland of 26 May 2023, Annex 5, para. 14.
[153] Reply by Microsoft Ireland of 26 May 2023, Annex 3, pp. 2 to 4, and Annex 6, pp. 2 to 4.
[154] Reply by Microsoft Ireland of 26 May 2023, Annex 3, pp. 2 to 4, and Annex 6, pp. 2 to 4.
[155] Reply by Microsoft Ireland of 26 May 2023, Annex 5, para. 14.
[156] Reply by Microsoft Ireland of 26 May 2023, Annex 5, para. 6.
[157] 2021 ILA, p. 8.

that is binding on the processor. Any documents that are not binding on Microsoft Ireland, including those issued by Microsoft to the Commission cannot satisfy the requirements of Article 29(3) of the Regulation. In particular, any explanation issued to the controller by the processor might potentially bind the processor only in so far as the processor does not choose to modify such an explanation. The EDPS is therefore of the view that any such explanation cannot be considered binding on the processor with regard to the controller within the meaning of Article 29(3) of the Regulation.

96. Similarly, the EDPS has seen no evidence that the 2021 DPIA, which was completed after the reference date, or parts of it are binding on Microsoft Ireland as the processor. Moreover, the data processing activities listed in section 3.10.2 of the 2021 DPIA are not linked to the terms used in the 2021 ILA and referred to in paragraph 90 of this decision. It is therefore not possible to attribute those activities to each of the purposes set out in the 2021 ILA.

97. The EDPS therefore considers that the Commission has failed to specify the purposes of "*ongoing improvement*", and in particular of "*making improvements to user productivity*",[158] to "*quality*"[159] and to "*efficacy*",[160] as required by Articles 4(1)(b) and 29(3) of the Regulation.

98. **Third**, it is unclear whether providing a particular online or professional service includes only "*troubleshooting*" in respect of that service or whether it includes troubleshooting in respect of other or all online or professional services respectively.

99. In its reply to the preliminary assessment, the Commission states that:

> "*The wording of the ILA does not allow Microsoft to process personal data for the purpose of troubleshooting and ongoing improvements for services to which the Commission does not subscribe to. First, for the sake of clarity, it is worth reminding that troubleshooting and ongoing improvements are part of the purposes of providing Customer the Online Services. Second, the ILA determines that Microsoft can process personal data* ***only*** *for identified set of purposes which are: 1) to provide Customer the Online Services 2) for Microsoft's business operations incident to delivery of the Online Services to Customer 3) for the purposes set out by EU or Member State law. Third, the ILA does not simply rely on that initial statement, but it even goes a step further by clarifying that 'where Microsoft is providing Online Services [...] except as permitted at law, [Microsoft] will not retain, use, or disclose that data for any purpose other than as set out in the DPA'. Fourth, an Online Service is defined in the ILA as follows 'a Microsoft-hosted service to which Customer subscribes under a Microsoft volume licensing agreement, including any service identified in the Online Services section of the Product Terms'.* [161]
>
> *As a result, Microsoft can only process personal data for troubleshooting and ongoing improvements purposes for a service that the Commission has subscribed to*

[158] Section on "*Processing to Provide Customer the Online Services*" in the main body of the DPA, 2021 ILA, p. 29.

[159] Section on "*Processing to Provide Customer the Professional Services*", Chapter 4, 2021 ILA, p. 65.

[160] Section on "*Processing to Provide Customer the Online Services*" in the main body of the DPA, 2021 ILA, p. 29, and section on "*Processing to Provide Customer the Professional Services*", Chapter 4, 2021 ILA, p. 65.

[161] Commission's reply of 25 May 2023, para. 37.

in the volume licensing agreement or when it has requested an online service identified in the Online Services section of the Product Terms."[162]

The EDPS concurs with the Commission's statement that, in principle, the 2021 ILA excludes "*troubleshooting*" which relates to services that the Commission does not subscribe to.[163] However, the EDPS considers that the evidence below demonstrates that Microsoft Ireland as the Commission's processor does not share such interpretation of the 2021 ILA.

100. In 2021, the Commission cited a letter[164] in which Microsoft stated that:

> "W*ith respect to 'troubleshooting', 'delivering functional capabilities' and 'online improvement', we confirm that this is linked to the Online Service provided, except where otherwise noted. The latter applies for troubleshooting, where the DPA talks about preventing, detecting, and repairing problems affecting the operation of Online Services. The latter is a more general reference, applying to other Online Services as well."*

101. In its reply to the preliminary assessment, the Commission states that:

> "*The reference to 'other Online Services' contained in the substantive reply of 7 June refers indeed to the online services identified in the Online Services section of the Product Terms.*"[165]

102. First, the EDPS understands the reference to the "*substantive reply of 7 June*" as a reference to the substantive reply of 15 October 2021, since only the latter refers to "*other Online Services*". This also corresponds to the Microsoft's letter cited by the Commission.[166]

103. Second, in the Microsoft's letter cited by the Commission,[167] Microsoft states that "*troubleshooting*" is linked to the "*Online Service **provided**, except where otherwise noted*" (emphasis added). The EDPS therefore understands that "*where otherwise noted*", troubleshooting is linked to online services that are *not provided*. According to Microsoft, this applies to preventing, detecting, and repairing problems affecting the operation of online services, with such online services being a "*more general reference*", applying to other online services as well. The EDPS therefore understands the cited letter as explaining that Microsoft can process personal data under the 2021 ILA to troubleshoot online services that are not provided to the Commission.

104. Third, the Commission's statement that "other Online Services" refers to the online services referred in the Online Services section of the Product Terms, is not consistent with the cited Microsoft's letter in which the term "other Online Services" is used.

---

[162] Commission's reply of 25 May 2023, para. 38.

[163] Under the DPA, "*troubleshooting*" includes "*preventing, detecting, and repairing problems affecting the operation of Online Services*" (2021 ILA, p. 29). "*Online Service*" under the DPA means "*a Microsoft-hosted service to which Customer subscribes under a Microsoft volume licensing agreement.*" (2021 ILA, p. 25).

[164] Commission's substantive reply of 15 October 2021, paras. 2.3.1.5 and 2.3.1.6, p. 7.

[165] Commission's reply of 25 May 2023, para. 38.

[166] Commission's substantive reply of 15 October 2021, paras. 2.3.1.5 and 2.3.1.6, p. 7.

[167] Commission's substantive reply of 15 October 2021, paras. 2.3.1.5 and 2.3.1.6, p. 7.

Instead, that letter demonstrates that "other Online Services" refers to services not provided to the Commission.

105. It follows that the purpose of "*troubleshooting*" under the 2021 ILA is not sufficiently clear for it to be understood in the same way by the Commission and Microsoft and is therefore not explicit and specified. This is in breach of Articles 4(1)(b) and 29(3) of the Regulation.

106. This conclusion is further supported by two mutually consistent facts. First, in the cited letter, Microsoft only referred to troubleshooting as being linked to services not provided, and did not refer to "*ongoing improvement*" in the same way.[168] Second, on 19 December 2023, the Commission and Microsoft Ireland concluded an amendment to the DPA, which, inter alia, changes the description of "*ongoing improvement*" as follows:

> *"Ongoing improvement (installing the latest updates and capabilities, and making improvement to user productivity, reliability, efficacy, and security of the Online Service* ***the Customer uses or subscribes to****)"* (emphasis added).[169]

107. The EDPS notes that the amendment does not modify the description of "troubleshooting" under the DPA, which remains described as "*preventing, detecting, and repairing problems affecting the operation of Online Services*". The EDPS considers that not adding the same qualification to the description of troubleshooting as was added to the description of ongoing improvement[170] is a further indication that troubleshooting which relates to services that the Commission does not use or subscribes to is construed by Microsoft as permitted under the 2021 ILA.

108. The conclusions of the EDPS referred to in paragraphs 88 to 107 are not undermined by the further information Microsoft Ireland has provided on these purposes in its reply to the preliminary assessment.

109. In particular, Microsoft Ireland states that:

> "*[...] Personal Data is processed within Microsoft, for features such as recording and transcribing the meeting or for translating chat messages [...]. [...] System Generated Logs are used for troubleshooting (preventing, detecting, and repairing problems), keeping products up to date and performant, and enhancing user productivity, reliability, efficacy, quality, and security*".[171]

According to Microsoft Ireland, infrastructure and platform logs[172], internal system

---

[168] The EDPS understands the reference to "*online improvement*" in the cited Microsoft's letter as a reference to "*ongoing improvement*" as there is no notion of "*online improvement*" in the 2021 ILA.

[169] Commission's email of 19 December 2023. Similarly also in the reply by Microsoft Ireland of 26 May 2023, Annex 5, para. 70.

[170] The EDPS understands that the objective of the amendment quoted in para. 106 was clearly to limit the ongoing improvement to services that the Commission uses or subscribes to. If indeed a reference to "Online Service" were to be sufficient, with respect to troubleshooting, to understand it as an online service that the Commission uses or subscribes to, this begs the question why it was decided and deemed necessary to make the addition solely with respect to ongoing improvement.

[171] Reply by Microsoft Ireland of 26 May 2023, Annex 6, p. 4.

[172] According to Microsoft, these logs "[aid] *capacity trending analysis*" and are "*required for Microsoft to provide and maintain baseline system operations*". Reply by Microsoft Ireland of 26 May 2023, Annex 3, pp. 3-4.

events logs[173], customer requests and server traffic logs[174] as well as customer event logs[175] may be recorded for operations and system heath logging purposes[176] and audit logging purposes[177]. Furthermore, "*a given log record may be used to achieve either or both of* [these] *purposes*".[178]

Giving the example of Teams, Microsoft Ireland further explains the purposes for which it processes other types of data:

> "*[...] to provide the Teams service and keep it secure, up to date and performing as expected",*[179] "*to power the services that provide application functionality, and information collected to enable the identification, classification, diagnosis, and remediation of issues*",[180] and "*to keep Teams secure and up to date and to detect, diagnose, and remediate problems, and make product improvements*"[181].[182]

The EDPS considers that these submissions contain information which to a limited extent clarifies certain purposes for which Microsoft processes certain personal data. However, these submissions do not provide information that could ensure that the purpose of the provision of online and professional services, as explained above, has been specified as required by the Regulation. In particular, it has not been demonstrated that this information has been set out in a contract or another binding act under EU or Member State law.

110. The EDPS therefore maintains that the purpose of the provision of online and professional services cannot be considered explicit and specified. The Commission has therefore infringed Article 4(1)(b) of the Regulation.

111. In the light of all of the above, the EDPS considers that a purpose set out in a contract signed under Article 29(3) of the Regulation which is not explicit and specified cannot

---

[173] According to Microsoft, "*these logs permit the monitoring of cloud service components to ensure the customer experience is not negatively impacted and to help diagnose and anticipate problems*", as well as to "*help Microsoft manage the security posture [...] and monitor performance trends at the software level*". Reply by Microsoft Ireland of 26 May 2023, Annex 3, p. 4.

[174] According to Microsoft, these exchanges of client/server traffic "*must be logged for security purposes*". According to Microsoft, they are also used to "[help] *Microsoft monitor the real-time experience our customers are having*", "*to reconstruct sequences of events and determine their outcome*" and "*to identify or investigate incidents and to monitor application usage for compliance and auditing purposes*". Reply by Microsoft Ireland of 26 May 2023, Annex 3, p. 4.

[175] According to Microsoft, "*customers need detailed insights about how their data is being used by their users and how their organization is using cloud resources*" and "*this class of logging enables a detailed audit log to be curated and provided to each customer*". Reply by Microsoft Ireland of 26 May 2023, Annex 3, p. 4.

[176] According to Microsoft, logs for this purpose are "*used to track events that are necessary to keep systems and services secure, performant, and up to date*". Reply by Microsoft Ireland of 26 May 2023, Annex 3, p. 2.

[177] According to Microsoft, logs for this purpose are "*used to track significant events in the system, either for Microsoft to meet its contractual obligations to customers or as a business requirement to support customers in meeting their own independent business and regulatory requirements*". Reply by Microsoft Ireland of 26 May 2023, Annex 3, p. 2.

[178] Reply by Microsoft Ireland of 26 May 2023, Annex 3, p. 2.

[179] According to Microsoft, this may include customer data.

[180] According to Microsoft, this concerns functional data, which are also required to exchange data with Optional Connected experiences.

[181] According to Microsoft, this concerns diagnostic data, which may contain pseudonymised personal data.

[182] Reply by Microsoft Ireland of 26 May 2023, Annex 6, p. 2.

be deemed to comply with that Article.[183] The Commission has therefore infringed Article 29(3) of the Regulation.

112. Accessorily, the EDPS notes that German data protection authorities have reached similar conclusions in their assessment of Microsoft 365 on how purposes of processing are insufficiently set out in the September 2022 Data Processing Agreement.[184] Other data protection authorities, such as the Greek and Lithuanian, have identified similar issues.[185]

Controllership status of Microsoft

113. Determining what types of personal data are to be processed is a part of the essential elements of the means of the processing. They are exclusively to be determined by the controller, together with the purposes of the processing, as provided for in Article 3(8) of the Regulation. The processor must not decide what types of personal data to process without the controller's approval. Together with the purpose of processing, the essential means are also closely linked to the question of whether the processing is lawful, necessary and proportionate. As the EDPB has stated, "*when a processor processes data outside or beyond the controller's instructions, and this amounts to a decision determining the purposes and means of processing, the processor will be in breach of its obligations and will even be considered a controller in respect of that processing in accordance with Article 28(10) [GDPR]*".[186]

114. In its preliminary assessment, the EDPS considered that since the Commission had not ensured that the purposes of processing in the context of providing online and professional services were explicit and specified, Microsoft itself determined those purposes to a significant extent. The EDPS considered that Microsoft therefore carried out such processing without sufficiently detailed instructions from the Commission as the controller. At least as regards the purposes and essential elements of the processing, such instructions are necessary in order to comply with Article 29(3)(a) of the Regulation.[187] The EDPS also considered that the Commission had left the decision as to when and how such processing may be carried out to Microsoft's discretion. The EDPS further considered that this did not comply with Article 30 of the Regulation in so far as Microsoft carried out processing activities without instructions from the controller.

115. In its reply to the preliminary assessment, the Commission states that:

> "*It has provided clear instructions to Microsoft with regard to the types of personal data and the purposes of the processing. The Commission considers that the*

[183] See also EDPB Guidelines 07/2020, para. 114, and the reasoning to that effect in section 3.1.2.1 of this decision.

[184] See the findings of the Conference of German DPAs on Microsoft Online Services (Microsoft 365), 24 November 2022, in summary (pp. 3, 4 and 5) and assessment (pp. 10, 11, 13, 14 and 15). See similarly the findings of the Baden-Württemberg DPA's audit of Microsoft 365 in the context of a pilot project on its possible use in schools (23 April 2021, published 25 April 2022), in particular in the Baden-Württemberg DPA's opinion (p. 6, 7, 8, 10 and 11).

[185] See in this respect the EDPB report on the 2022 Coordinated enforcement action on the use of cloud-based services by the public sector, 17 January 2023, in particular findings by the Greek and Lithuanian DPAs in annex (pp. 50, 51, 53, 95 and 96).

[186] See also EDPB Guidelines 07/2020, paras. 30, 40, 80, 84 and 117.

[187] EDPB Guidelines 07/2020, paras. 112, 114, 116 to 118.

contractual instructions provided to Microsoft include all of the elements mentioned under article 29(3) of the Regulation and as these are further described in the EDPB Guidelines 07/2020. The Commission requests the EDPS to further elaborate the statement 'Microsoft itself determines those purposes to a significant extent'. It is unclear which purposes the EDPS refers to and the extent to which Microsoft determines them.".[188]

As regards the lack of instructions pertaining to the purposes and essential means of the processing, the EDPS refers to its conclusions set out in paragraphs 110 and 111, and the underlying reasoning preceding those paragraphs. The EDPS also considers that the Commission's quoted statement does not provide any new relevant arguments against those conclusions that have not already been responded to above. The EDPS is of the view that since the purposes referred to in paragraphs 88 to 106 have not been explicit and specified, Microsoft Ireland as the Commission's processor is permitted to compensate for that failure by determining them itself. This is inherent, in principle, in any situation where the controller does not ensure that the purposes are explicit and specified. One of the main objectives of the principle of purpose limitation is to ensure that the processor does not 'fill in the gaps' resulting from insufficiently explicit and specified purposes of the processing. Indeed, that principle requires that the purposes are made explicit and specified by the controller.[189]

116. In this regard, Microsoft Ireland states that:

"It is not reasonable to expect a Microsoft customer, such as the Commission, that is relying on Microsoft to provide secure, efficient and robust and globally enabled services, to in turn provide detailed instructions to that cloud provider on how to run its core business. This exposes both the Commission and Microsoft to risk – from a cyber, IT and data protection security perspective. For this exact reason, EU data protection law does not require data processing agreements or instructions to be set out with a high level of granularity, and data protection authorities have maintained that processors, in particular those who are highly sophisticated, should still have sufficient discretion to determine the 'non-essential' means of processing – as long as the controller retains control over the 'essential' processing purposes."[190]

"When engaging a robust and globally enabled cloud service provider, there is no requirement on the controller (i.e. the Commission) to have the same full level of technical understanding of the functioning of the data processing service as the processor (i.e. the cloud service provider). The customer's general understanding of

[188] Commission's reply of 25 May 2023, para. 65.

[189] Taking into account the GDPR and the relevant case-law, the EDPB has in a similar vein stated in para 101 of the EDPB Binding Decision 5/2022: "*The GDPR makes WhatsApp IE, as the controller for the processing at stake, directly responsible for complying with the GDPR's principles, including the processing of data in a lawful, fair and transparent manner, and any obligations derived therefrom. This obligation applies even where the practical application of GDPR principles such as those of Article 5(1)(a) and Article (5)(2) GDPR are inconvenient or run counter to the commercial interests of WhatsApp IE. The controller is also obliged to be able to demonstrate that it meets these principles and any obligations derived therefrom, such as that it meets the specific conditions applicable to each legal basis.*" See, to that effect, also para. 105 of the EDPB Binding Decision 3/2022 and para. 108 of the EDPB Binding Decision 4/2022.

[190] Reply by Microsoft Ireland of 26 May 2023, para. 361; see also para. 193.

the processing activities is legally sufficient – and the processor's technical expertise does not convert it into a controller under the EUDPR."[191]

"It is market practice for comprehensive and dynamic data processing services such as cloud services, to be described in general contractual language – as describing it in overly granular detail would impose unreasonable and counterproductive burdens on the contractual parties – including because sensitive and ever-improving cybersecurity measures cannot be fully captured in any static set of contracts or public statements, for the very reason that it exists, to protect the parties from bad actors when the data processing details are highly dependent on the data fed into the M365 services by the customer and its users, which changes frequently." [192]

The EDPS does not consider that those statements demonstrate that the Commission has given Microsoft Ireland sufficiently detailed instructions to comply with Article 29(3)(a) of the Regulation, for the following reasons.

117. Indeed, the EDPS and the EDPB both consider that the processor may determine the non-essential means of the processing while the controller must determine the purposes and essential means of the processing.[193] The EDPS does therefore not object to the possibility of Microsoft Ireland determining non-essential means of the processing, such as the choice for a particular type of hard- or software or the detailed security measures or other practical aspects of implementation.[194] However, in this decision, the EDPS has found that the Commission has not determined the types of personal data, which fall under essential means of the processing, the purposes of the processing, as required by the Regulation. Under the Regulation, the types of personal data and purposes must always be determined by the controller which must give sufficient instructions in this regard.[195] In this regard, there is also no distinction, as suggested by Microsoft Ireland,[196] between essential and non-essential purposes of the processing. All purposes of the processing must be determined by the controller.

118. The EDPS acknowledges that a processor may in many instances have a higher level of technical expertise than the controller.[197] This does not, however, imply that the controller does not need to comply with Articles 4(1)(b) and 29(3)(a) of the Regulation, in particular as regards the determination of the purposes of the processing and types of personal data and related instructions. As rightly noted by Microsoft Ireland in its reply to the preliminary assessment,[198] instructions and even wording for the contract between the controller and processor may be suggested by the processor, as long as they are accepted by the controller.[199] However, as explained above, the EDPS has not seen evidence that would demonstrate that instructions were suggested by Microsoft Ireland and accepted by the Commission that would ensure that the purposes of processing and types of personal data have been determined as required by the Regulation. Moreover,

---

[191] Reply by Microsoft Ireland of 26 May 2023, para 182.
[192] Reply by Microsoft Ireland of 26 May 2023, para. 182, footnote 106.
[193] EDPB Guidelines 07/2020, para. 40.
[194] EDPB Guidelines 07/2020, para. 40.
[195] See Articles 3(8) and 29(10) of the Regulation.
[196] Reply by Microsoft Ireland of 26 May 2023, para. 361.
[197] The EDPS nonetheless underlines the status of the Commission as a controller under the Regulation that carries out tasks in the public interest and is responsible for the processing of personal data of tens of thousands of data subjects (see para. 74 of this decision).
[198] Reply by Microsoft Ireland of 26 May 2023, paras. 185 to 187.
[199] EDPB Guidelines 07/2020, para. 116.

any market practice that does not comply with the law cannot be deemed acceptable and compliant merely because it might be widespread.[200] [201]

119. The DPA provides that the following documentation constitutes the Commission's documented instructions:

> "*[The Commission] agrees that its volume licensing agreement (including this DPA and the Product Terms Site), along with the product documentation and Customer's use and configuration of features in the Online Services, are Customer's* ***complete documented instructions*** *to Microsoft for the processing of Personal Data*" (emphasis added).[202]

The Commission can therefore give documented instructions only via the indicated documents or configuration settings,[203] including via the Product Terms Site.[204] However, in its reply to the preliminary assessment, Microsoft Ireland has stated that the following should also be "*taken into account when it comes to the controller's instructions:*

> *[…] other communications and the various meetings held by the Commission and Microsoft where the Commission was given the opportunity to issue additional instructions or specify its instructions further".*[205]

In order to ensure proper understanding of that statement, the EDPS has invited the Commission and Microsoft Ireland to explain how instructions given via "*other communications*" and "*at various meetings held by the Commission and Microsoft*" fall within the complete documented instructions provided for by ILA.[206] Microsoft Ireland has replied to that question at the hearing of 23 October 2023. It has stated that:

> *"The [quoted statement[207]] should be understood as meaning that the Commission's instructions […] are set out in writing in the various documents referenced in the ILA 2021. That is the ILA itself, the Microsoft Product Terms Site, product documentation,* the Commission's use and configuration of features in the online services, and ***are further specified and explained through oral meetings and other communications.*** *(emphasis added)"*

The EDPS understands that the documents defined in the 2021 ILA as complete documented instructions may therefore be further specified and explained through oral meetings and other communication. Such specification of documented instructions is

---

[200] With regard to the required level of granularity of the determination of the purposes of the processing and types of personal data, and related instructions, see, in particular, para. 92 of this decision.

[201] See also para. 105 of the EDPB Binding Decision 3/2022, para. 108 of the EDPB Binding Decision 4/2022 and para. 101 of the EDPB Binding Decision 5/2022.

[202] Section on "*Processor and controller Roles and Responsibilities*" in the main body of the DPA, 2021 ILA, p. 31.

[203] To the extent that any such configuration settings for Microsoft 365 set by the Commission are documented and are not reversed or otherwise changed by Microsoft.

[204] Under the DPA (2021 ILA, p. 26), the Product Terms Site are found at: https://www.microsoft.com/licensing/terms/product/PrivacyandSecurityTerms/EAEAS. Under the DPA, Microsoft can change the Product Terms Site when it introduces new features, supplements or related software. However, the Commission is free to refuse such features with no loss to existing functionality (2021 ILA, pp. 24-25).

[205] Reply by Microsoft Ireland of 26 May 2023, para. 186.

[206] EDPS' letter to the Commission of 28 July 2023, Annex 2, para. 7 and question F.

[207] Reply by Microsoft Ireland of 26 May 2023, para. 186.

not envisaged under the 2021 ILA. Moreover, in view of the exhaustive nature of the list of documents contractually provided for as documented instructions, such specification does not appear to be allowed. In any event, neither Microsoft Ireland nor the Commission have explained or otherwise demonstrated how instructions given at oral meetings are documented. The EDPS therefore considers that some of the instructions are provided by the Commission in breach of the 2021 ILA, without clear demonstration that they are documented.

120. In addition to that, Microsoft Ireland had proposed an amendment to the 2021 ILA,[208] which was, in a somewhat modified form, concluded on 19 December 2023,[209] and which, inter alia, introduced a more limited number of business operations purposes. When referring to the content of the amendment proposal, Microsoft Ireland stated that:

> "*This is something that is not yet finalised in the contract, but what the contract would be doing would be applying what we're already doing in practice*".[210]

The EDPS therefore finds that, prior to the amendment of 19 December 2023, Microsoft Ireland was carrying processing operations in a way that was inconsistent with the applicable ILA. The EDPS understands this to be another indication that Microsoft Ireland does not in all circumstances consider the Commission's instructions to it, both contractual and non-contractual, as binding.

121. In view of the above,[211] the EDPS maintains its findings as set out in paragraph 114. The Commission has not given adequate instructions to Microsoft Ireland, in particular as regards the purposes and types of personal data. The Commission has therefore failed to ensure that Microsoft only processes personal data on the Commission's documented instructions and has thus allowed Microsoft to determine the purposes and means of the processing. Under Article 29(10) of the Regulation, Microsoft must therefore be considered a controller in respect of that processing.[212]

122. Under Article 26(1) of the Regulation, 'the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation'.

123. The controller's obligation under Articles 4(2) and 26(1) of the Regulation to be able to demonstrate compliance with the Regulation for any processing of personal data is not limited to processing carried out by the controller but also extends to processing on the controller's behalf.[213] The Commission has infringed Articles 4(2) and 26(1) of the Regulation in conjunction with Article 30 of the Regulation since it has not ensured that Microsoft only carries out processing on the Commission's behalf and its documented instructions as a controller. By not providing sufficiently clear documented instructions, the Commission has also infringed Article 29(3)(a) of the Regulation.

---

[208] Reply by Microsoft Ireland of 26 May 2023, Annex 5, para. 45.
[209] Commission's email of 19 December 2023.
[210] Statement by Microsoft Ireland at the hearing of 23 October 2023.
[211] Paras. 45 to 120 of this decision.
[212] See, to that effect, judgment in Case C-807/21, *Deutsche Wohnen*, para. 41, judgment in Case C-683/21, *Nacionalinis visuomenės sveikatos centras*, ECLI:EU:C:2023:949, para 30, and judgment in Case C-25/17, *Jehovan todistajat*, EU:C:2018:551, paras. 67 and 68. See in this respect also the EDPB report on the 2022 Coordinated enforcement action on the use of cloud-based services by the public sector, 17 January 2023, in report (pp. 15 and 30) and annex (pp. 76, 77, 102, 105 and 106).
[213] See recital 45 of the Regulation.

3.1.2.3. Processing for business operations

124. On 19 December 2023, the Commission and Microsoft Ireland concluded an amendment to the DPA which provides that:

> ***„For purpose of these „Microsoft's business operations", Customer instructs Microsoft:***
>
> ***i. to calculate aggregated non-personal numerical statistics from data containing either no identifiers at all or only pseudonymized identifiers (such as usage logs containing unique, pseudonymized identifiers); and***
>
> ***ii. to calculate non-personal numerical statistics related to Customer Data (without accessing or analysing the content of Customer Data)***
>
> ***in each case limited to achieving the purposes above, each as incident to providing the Online Services to Customer.***
>
> *When processing for Microsoft's business operations, Microsoft* ***will apply principles of data minimization and will*** *not use or otherwise process Customer Data or Personal Data for: (a) user profiling, (b) advertising or similar commercial purposes,* ***or (c) any other purpose, other than*** *the purposes set out in this section. Access to content of Customer Data is not permitted for business operations processing. When processing for Microsoft's business operations, Microsoft de-identifies the data. The process Microsoft uses to de-identify the data is compatible with Customer's purposes of processing under Article 6 EUDPR. The aggregation Microsoft performs follows the definition of aggregated data in ISO/IEC 19944, and the resulting data does not retain individual-level data (and thus is not Personal Data).*
>
> ***The processes referred in point (i) and (ii) above are carried out by Microsoft in accordance with the state of the art. At Customer's request, Microsoft will provide Customer with technical documentation describing how the processes described in (i) and (ii) are carried out in compliance with Microsoft's obligations under this clause. In addition, as with all processing under this DPA, processing for business operations remains subject to Microsoft's confidentiality obligations and commitments under Disclosure of Processed Data.***" (emphasis as included in the original text of the amendment marks parts that are new or changed compared to the previous version of the DPA)[214]

The EDPS notes that Microsoft Ireland stated at the hearing of 23 October 2023 that "*the [amendment] would be [...] applying what we're already doing in practice*"[215] and that the Commission has stated that the "*changes do not introduce new or fundamentally different processing operations*".[216] The EDPS therefore understands that the wording of

[214] Commission's email of 19 December 2023, Annex 2 (Amendment to Contract Documents), pp. 1 and 2, point 2; see as well similar amendments for software and professional services, respectively, on pp. 4 and 5, point 7, and pp. 5 and 6, point 9.

[215] Statement by Microsoft Ireland at the hearing of 23 October 2023.

[216] Commission's email of 19 December 2023.

amendment of 19 December 2023 reflects the factual situation, as regards processing for Microsoft's business purposes, already as of the reference date.

125. It follows from the wording of the amendment that only **non-personal data** are to be processed for Microsoft's business purposes. Microsoft Ireland has also made statements to this effect in its reply to the preliminary assessment in which it has presented, at the time, an amendment proposal.[217] In particular, Microsoft Ireland has stated that "*to perform these business operations, Microsoft processes only aggregated or statistical numerical non-personal data that does not directly link to any individual*".[218] Similarly, the Commission has stated that: "*The combination of pseudonymisation and aggregation results in the data handled by the data importer to become non-personal data rendering re-identification impossible.*"[219] According to those statements and the amendment of 19 December 2023, that aggregated statistical data created from pseudonymised data as well as statistics related to customer data and professional services data are claimed not to be 'personal data' as defined by the Regulation.

126. The EDPS must therefore assess whether the data concerned are indeed effectively anonymised, as put forward by the Commission and Microsoft Ireland, or whether they are to be considered personal data within the meaning of the Regulation.

Assessment of the alleged anonymisation

127. Article 3(1) of the Regulation states that 'personal data' must be understood as meaning 'any information relating to an identified or identifiable natural person', that is to say relating to a 'natural person [...] who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person'.[220]

128. It follows from recital 16 of the Regulation and from the definition of the concept of 'personal data' provided in Article 3(1) of the Regulation that neither 'anonymous information, namely information which does not relate to an identified or identifiable natural person', nor 'personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable', is covered by that concept. By contrast, it follows from Article 3(6) of the Regulation, read in conjunction with recital 16 of the Regulation, that personal data which have undergone pseudonymisation and which could be attributed to a natural person by the use of additional information must be considered to be information on an identifiable natural person, to which the principles of data protection apply.[221]

---

[217] Reply by Microsoft Ireland of 26 May 2023, Annex 5, para. 45.
[218] Reply by Microsoft Ireland of 26 May 2023, Annex 5, para. 45.
[219] Commission's reply of 25 May 2023, para. 145.
[220] See also recital 18 of the Regulation, which states that: 'Natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags. This may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them.'
[221] See, to that effect, judgment in Case C-683/21, *Nacionalinis visuomenės sveikatos centras*, ECLI:EU:C:2023:949, paras. 53, 57 and 58, as well as judgment in Case C-319/22, *Gesamtverband Autoteile-Handel (Accès aux informations sur les véhicules)*, ECLI:EU:C:2023:837, paras. 45 to 50.

129. As per settled case-law, information constitutes personal data where, by reason of its content, purpose or effect, the information in question is linked to a particular natural person. In order to determine whether a natural person is identifiable, directly or indirectly, account should be taken of all the means likely reasonably to be used either by the controller, or by any other person, to identify that person, without, however, requiring that all the information enabling that person to be identified should be in the hands of a single entity.[222] According to the Regulation, to demonstrate successful anonymisation, the controller must be able to show that data which are at the origin personal have been processed in such a way that they can no longer be used to identify a natural person either directly or indirectly, using all the means reasonably likely to be used either by the controller or a third party.[223]

130. In the assessment of the alleged anonymisation, the EDPS takes the perspective of the controller under the 2021 ILA (i.e. the Commission) and, in particular, of Microsoft, including both Microsoft Ireland and Microsoft Corporation.

131. In its reply to the preliminary assessment, Microsoft Ireland states that "*the underlying, unaggregated pseudonymous data remains available to the customer*".[224] Similarly, Microsoft has previously stated that it "*must maintain that underlying pseudonymous data to provide the services the EUIs have requested*".[225] Under the 2021 ILA, both before and following its amendments, Microsoft may retain all personal data (including pseudonymous data) it processes on behalf of the Commission until it stops providing services related to the processing, with the exception of customer data stored in each online service.[226] It follows that after the creation of the aggregated data, Microsoft does not delete the underlying pseudonymised or non-pseudonymised personal data.

132. According to the Article 29 Working Party's Opinion 05/2014, the robustness of an anonymisation techniques is based on three criteria:

    a) is it still possible to single out an individual (singling out),
    b) is it still possible to link records relating to an individual (linkability) and
    c) can information be inferred concerning an individual (inference).[227]

133. Singling out, linkability and inference are therefore means that can be used to identify a natural person directly or indirectly.[228]

134. As stated in the Opinion, linkability and inference remain a risk also after the aggregation of the data.[229] In addition, statistics would qualify as anonymous data only if they were aggregated to a level where the individual events are no longer identifiable and the underlying raw data were deleted.[230] As explained in paragraphs 131, 148 and

---

[222] Judgment in Case C-319/22, *Gesamtverband Autoteile-Handel (Accès aux informations sur les véhicules)*, ECLI:EU:C:2023:837, para 45.
[223] See recital 16 and Article 3(1) of the Regulation.
[224] Microsoft's reply of 26 May 2023, Annex 4, p. 10, fourth para.
[225] Microsoft's letter to the Commission of 15 April 2020, p. 4.
[226] 2021 ILA, p. 39.
[227] Article 29 Working Party's Opinion 05/2014 on Anonymisation Techniques, pp. 3, 11 and 12. The Article 29 Working Party also stated (on p. 9) that "*an effective anonymisation solution prevents all parties from singling out an individual in a dataset, from linking two records within a dataset (or between two separate datasets) and from inferring any information in such dataset*".
[228] See also recitals 16 and 18 of the Regulation.
[229] Article 29 Working Party's Opinion 05/2014, pp. 16, 17 and 24.
[230] Article 29 Working Party's Opinion 05/2014, p. 9.

157 of this decision, Microsoft does not delete the underlying data since it retains both non-pseudonymised and pseudonymised personal data after the aggregation.

135. In this regard, Microsoft Ireland has stated in its Business Operations White Paper that customers authorise Microsoft to:

> "*(i) process their personal data already generated in providing the services to create aggregated statistical, non-personal data from data containing pseudonymized identifiers (such as usage logs containing unique, pseudonymized identifiers) and*
>
> *(ii) calculate statistics related to Customer Data or Professional Services Data (both as defined in the DPA) for the four business operation purposes identified above,*
>
> *in each case without accessing or analyzing the content of Customer Data or Professional Services Data and limited to achieving only the enumerated purposes*".[231]

This text is similar, however not identical to the amendment of 19 December 2023.[232] With regard to the latter, the Commission has stated that: "*The changes do not introduce new or fundamentally different processing operations and therefore, by [its] understanding, no new facts to the investigation*".[233] Moreover, Microsoft Ireland has stated at the hearing of 23 October 2023 that the amendment proposal, which is, in essence, identical to the quote from the Business Operations White Paper above, "*is something that is not yet finalised in the contract, but what the contract would be doing would be applying what we're already doing in practice*".[234] The EDPS therefore considers that the arguments put forward by Microsoft Ireland in relation to the quoted text can be understood as applying fully also to the text of the amendment of 19 December 2023.

136. In view of the above, the EDPS invited the Commission and Microsoft Ireland to make known their views on, inter alia, the following questions, in order to better understand their replies to the preliminary assessment regarding the anonymisation of the data in question:

> "*Could you please explain and demonstrate how the calculation referred to in point ii) of paragraph [135 of this decision] is carried out and how it relates to customer data and professional services data?*
>
> *Could you please explain and demonstrate, separately for each of the following two points, how Microsoft ensures that the aggregated data and statistics referred to in points i) and ii) of paragraph [135 of this decision], respectively, cannot be used to identify a natural person either directly or indirectly (including by linking or inferring, from a single data set or several data sets), taking into account all the means reasonably likely to be used by Microsoft Corporation or another third party?***"**[235]

---

[231] Reply by Microsoft Ireland of 26 May 2023, Annex 4, page 7, point 2.
[232] Compare with para. 124 of this decision.
[233] Commission's email of 19 December 2023.
[234] Statement by Microsoft Ireland at the hearing of 23 October 2023.
[235] EDPS' letter to the Commission of 28 July 2023, Annex 2, paras. 1 to 4, questions A and D.

137. The Commission and Microsoft Ireland chose not to provide a written reply. However, Microsoft Ireland has provided the following explanations in this regard at the hearing of 23 October 2023.

> "Aggregated statistical, non-personal data from data containing pseudonymized identifiers" [236]

138. With regard to point i) quoted in paragraph 135 of this decision (concerning "*aggregated statistical, non-personal data from data containing pseudonymized identifiers*"), Microsoft Ireland has stated at the hearing of 23 October 2023 that:

> "*To the extent aggregated statistical data for business operations are created from data containing identifiers, those identifiers are all pseudonymised. [...] It doesn't contain any data related to an individual user. It's an overall count. [...] The primary use always of the data* [from logs generated by Microsoft 365 services] *is for operations of the service. [...] Before they are used for business operations processing, however, they are scrubbed, aggregated, and de-identified [...] and anonymised.*"[237]

139. At the hearing of 23 October 2023, Microsoft Ireland has further stated that Microsoft and the system take "***preventive measures and detective measures*** *[...] to ensure that the data used to calculate statistics for business operations do not contain identifiers unless they are pseudonymised*".[238] Moreover, the "*second step [...] is the aggregation resulting [in] the underlying data for the reports"* for business operations.[239]

140. As regards "**preventive measures**" implemented by Microsoft, Microsoft Ireland has provided the following explanations at the hearing of 23 October 2023.

141. Microsoft Ireland has presented at the hearing "*a sample of a copy and a delete action from a user*" as an example of a "*log that contains [...] individual pseudonymised identifiers, which are hexadecimal pseudonymised identifiers*".[240] It has stated that "*logs that contain a reference to the user ID always use the pseudonymised user ID*" and that "*logs, when they are created, do not contain directly identifiable information to the specific user, the data subject*". Microsoft Ireland has also presented an example of "*a pseudonymised identifier when a new user is created in the system*".[241] It has stated that "*that pseudonymised identifier [listed as object ID] is created at the moment that user is registered*" and that "*the source mapping for these pseudonymous identifiers is stored*

---

[236] See point i) quoted in para. 135 of this decision. The EDPS understands that this in essence corresponds to the amendment of 19 December 2023 quoted in para. 124, point i), of this decision.

[237] Statement by Microsoft Ireland at the hearing of 23 October 2023. See also letter by Microsoft Ireland of 24 October 2023, Business Operations visuals [slides presented at the hearing of 23 October 2023], pp. 4 and 10 for an example of statistics of "*the monthly active user count of* ***European Commission*** *for the application Teams*" (emphasis added) which Microsoft Ireland presented at the hearing. According to Microsoft Ireland, the code counts the number of users using Teams [from raw data in logs] resulting in an aggregate number of premium users and standard users in the overall user count. Microsoft Ireland, has also stated at the hearing that "*this report only shows [...] how many end users at a particular tenant, in this case the* ***Commission****, have used Teams in a given month*" (emphasis added).

[238] Statement by Microsoft Ireland at the hearing of 23 October 2023.

[239] Statement by Microsoft Ireland at the hearing of 23 October 2023.

[240] See letter by Microsoft Ireland of 24 October 2023, Business Operations visuals [slides presented at the hearing of 23 October 2023], p. 5.

[241] See letter by Microsoft Ireland of 24 October 2023, Business Operations visuals [slides presented at the hearing of 23 October 2023], p. 6.

within the EU as part of the EU data boundary and is subject to multiple layers of protections against re-identification".[242]

142. Based on an architecture diagram,[243] Microsoft Ireland has presented, at the hearing of 23 October 2023, how the scrubbing takes place in three phases within the system:

> "*The scrubbing service [...] either deletes the personal data entirely, or only when Microsoft has a specific use case where it needs to pseudonymise identifiers for counting, for example, then it will pseudonymise that data using a key-hashed message authentication code, HMAC mechanism*[244]*, to pseudonymise those fields. [...] It takes data from the service* [and] *scans that data for any personal data. Then it goes to the transform stage, and the transformer takes any found personal data, then scrubs it, so either deletes it from that data, or it uses that HMAC mechanism to pseudonymise. So it replaces the original field with the pseudonymous identifier. [...] The third phase [is] the dumper, [...] that stores the resulting data set into the storage that's used for longer term data log storage [(the data destination)]. [...] HMAC [is] based on NIST FIPS 198-1*[245]*, and we use HMAC SHA-256*[246] *as the mechanism, and SHA-256 is also an ISO standard [...] 10118-3:2016.*[247]"
>
> At the hearing, Microsoft Ireland has also presented an example of a "*log [that contained], when it was created, [...] a MAC address of the device that would have been used by a user and the IP address [of the device that would have been used]*".

---

[242] Statement by Microsoft Ireland at the hearing of 23 October 2023.

[243] See letter by Microsoft Ireland of 24 October 2023, Business Operations visuals [slides presented at the hearing of 23 October 2023], p. 7.

[244] HMAC is sometimes expanded as either keyed-hash message authentication code or hash-based message authentication code. In cryptography, an HMAC is a specific type of message authentication code (MAC) involving a cryptographic hash function (algorithm) and a secret cryptographic key. As with any MAC, it may be used to simultaneously verify both the data integrity and authenticity of a message. Without the knowledge of this key, it is computationally infeasible to map the identifiers and the pseudonyms. The cryptographic strength of the HMAC depends upon the size of the secret key that is used and the security of the underlying hash function (algorithm) used. Computational infeasibility depends on the specific security requirements and environment. One meaning, commonly used by security practitioners, of the computational infeasibility is that it cannot be computed practically with generally available resources in a reasonable amount of time. Techniques for computing a MAC using a hash function are specified in standard ISO/IEC 9797-2 Information technology – Security techniques – Message Authentication Codes (MACs) – Part 2: Mechanisms using a dedicated hash-function (latest published version of this standard is ISO/IEC 9797-2:2021, with a technical corrigendum ISO/IEC 9797-2:2021/CD Cor 1 under development).

[245] National Institute of Standards and Technology (US Department of Commerce), Federal Information Processing Standard 198-1 on The Keyed-Hash Message Authentication Code (HMAC). Available at https://csrc.nist.gov/pubs/fips/198-1/final. In November 2022, NIST decided to revise the text of FIPS 198-1 standard and convert it to NIST Special Publication 800-224 and to withdraw FIPS 198-1 when NIST SP 800-224 is published (https://csrc.nist.gov/news/2022/decision-to-convert-fips-198-1-to-nist-special-pub). See also information note describing HMAC (IETF RFC 2104, as updated by RCF 6151), issued by the Internet Engineering Taskforce.

[246] Hash-based Message Authentication Code Secure Hash Algorithm 256-bit. SHA-256 (part of the SHA2 family) is one of the secure hash algorithms specified by NIST in NIST FIPS 180-4 standard. Secure hash algorithms are typically used with other cryptographic algorithms. The security guidelines recommended by NIST when using secure hash algorithms (such as SHA-256) in cryptographic applications that employ hash functions (algorithms) such as HMAC are provided in NIST SP 800-107 Rev. 1 and when the HMAC keys are generated are provided in NIST SP 800-133 Rev. 2.

[247] Latest published version of this standard under review is ISO/IEC 10118-3:2018 IT Security techniques – Hash-functions – Part 3: Dedicated hash-functions. The hash-functions specified in the ISO/IEC 10118 series of standards (all parts) do not involve the use of secret keys. However, these hash-functions may be used, in conjunction with secret keys, to build message authentication codes. See, in this respect, footnote 244 of this decision.

It has stated that "*both [are] considered personal data, and therefore picked up by this scrubbing service [...], and transformed [using the HMAC mechanism] into pseudonymous identifiers [...]*".[248] It has also stated that "*this is actually being stored in [Microsoft's] data log storage*", that the "*preventive measures [...] operate automatically on [Microsoft's] systems*" and that "*the system actively pseudonymised identifiers, [such as] the [unique user ID] UUID, the object ID [and] the pseudonymised ID.*"[249]

143. As regards "**detective measures**" used by Microsoft, Microsoft Ireland has provided the following explanations at the hearing of 23 October 2023.

144. As a first class of detective measures, Microsoft Ireland has explained at the hearing that they use automatic source code validation as part of Microsoft's Secure Development Lifecycle. Microsoft Ireland has stated that "*an auto-reviewer tool*" scans through the source code being generated by Microsoft's engineers and developers to create logs "*for any mistakes* [in the code that would result in] *any personal data end[ing] up without being scrubbed.*"[250]

145. As a second class of detective measures, Microsoft Ireland has explained at the hearing that they use detective controls which look at the outcome, where "*the detector [...] filters through the output [from the scrubber] and validates again whether all personal data that is remaining in the output is really scrubbed successfully [...] and [...] whether the outcome is according to [Microsoft's] policy and [...] according to the agreements with [Microsoft's] customers*".[251]

146. Microsoft Ireland has also referred, at the hearing, to internal processes carried out "*before [Microsoft] use[s] or allow[s] the use of [those] pseudonymised logs to start working on preparing [...] a new data set for business operations*". It has stated that: "*That begins with several approval and validation requirements to verify that the requested report by a business operations function within Microsoft or statistics fit within an agreed business operations purpose. [...] Some of these requirements include a privacy review, an in-depth privacy review of the scenario being requested, a legal review, several approvals and sign-off*".[252]

147. At the hearing of 23 October 2023, Microsoft Ireland has also stated that "*data used for business operations reports does not contain personal data, and thus Microsoft implements*

[248] See letter by Microsoft Ireland of 24 October 2023, Business Operations visuals [slides presented at the hearing of 23 October 2023], p. 8.

[249] Statement by Microsoft Ireland at the hearing of 23 October 2023.

[250] Statement by Microsoft Ireland at the hearing of 23 October 2023. See letter by Microsoft Ireland of 24 October 2023, Business Operations visuals [slides presented at the hearing of 23 October 2023], p. 9. The EDPS understands that Microsoft uses this "*first class of detective measures*" is used at the beginning of the software development process.

[251] Statement by Microsoft Ireland at the hearing of 23 October 2023. See letter by Microsoft Ireland of 24 October 2023, Business Operations visuals [slides presented at the hearing of 23 October 2023], p. 7, "Detector" field in the architecture diagram. The EDPS understands that Microsoft uses this "second class of detective measures" once the Microsoft software is in production and the logs and other data are being collected. The EDPS understands that the detector checks after the scrubbing process (which is preventive measure) whether the scrubbing (pseudonymisation) was successful.

[252] Statement by Microsoft Ireland at the hearing of 23 October 2023.

and adheres to ISO standard ISO-19944[253] *concerning aggregation*".[254] It has further stated that:

> *"The aggregated data and statistics metrics do not contain any personal data, and even when one would gain access to the underlying data source, there is nothing that can be inferred or re-engineered, because the underlying data source used for this report is aggregated and based on all the mechanisms [...] just explained."*[255]

148. Similarly, in its reply to the preliminary assessment, Microsoft Ireland made the following statements in relation to pseudonymisation and aggregation:

> "*It is important to understand that, for the majority of these purposes, Microsoft only needs to process Diagnostic Data in pseudonymized form – and so it does not process this Diagnostic Data in non-pseudonymized form (i.e., the data will not reveal that for User named John Doe at the Commission's app have crashed – they will only reveal that 'for User 12345678', the Teams app crashed 5 times in 1 day and 30 times the last month).*[256] *[...] Diagnostic Data is pseudonymized – meaning direct identifiers are removed and replaced with unique IDs (numeric codes).*[257] *[...] The only Personal Data processed by Microsoft in non-pseudonymized form throughout all stages of processing under the 2021 ILA is Customer Data for providing the service. All other data is either pseudonymized – as in Service-Generated Data, which is pseudonymized before transfer and storage, and Diagnostic Data – or aggregated – as data used for business operations. Microsoft aggregates the data in line with the ISO/IEC 19944 standard.*"[258]
>
> "*Microsoft uses various techniques to pseudonymize personal data in system-generated logs, including encryption, masking, and tokenization.*"[259]
>
> "*Microsoft mitigates the risk to the privacy of data subjects by using privacy by default and by design. Microsoft operates to a design policy that system logging software must substitute identifiable personal data from Customer Data with pseudonyms or tokens. This can be done when the log record is recorded or can be done as a follow-up substitution (aka pseudonymization) process. [...] There are a variety of ways substituted tokens used to pseudonymize personal data in log records can be generated. The substituted token may be cyphertext generated by cryptographic means (e.g., a nonreversible hash) or a computed unique identifier or simply just a plain-text alphanumeric token pulled in sequence from a constantly growing table of preallocated pseudonymization tokens. The crucial thing is that if pseudonym substitution is being conducted, the 'additional information' that would re-identify the pseudonym (such as a cypherkey, user IDs, email addresses) must be stored apart from the pseudonymized record and not made available to personnel who work with the pseudonymized record. Accordingly, Microsoft limits access to token look-up tables as for Customer Data. [...]*

---

253 ISO/IEC 19944 Cloud computing and distributed platforms — Data flow, data categories and data use. Latest published version of this series of standards is ISO/IEC 19944-1:2020 and ISO/IEC 19944-2:2022.

254 Statement by Microsoft Ireland at the hearing of 23 October 2023.

255 Statement by Microsoft Ireland at the hearing of 23 October 2023.

256 Reply by Microsoft Ireland of 26 May 2023, Annex 5, para. 77.b.

257 Reply by Microsoft Ireland of 26 May 2023, Annex 5, para. 95.

258 Reply by Microsoft Ireland of 26 May 2023, Annex 5, para. 106. See also reply by Microsoft Ireland, para. 56 and footnote 101 on p. 53.

259 Reply by Microsoft Ireland of 26 May 2023, Annex 3, p. 6, second para.

After the generation of statistics and aggregation of data from the input data, all business operations processing is limited to using statistics and aggregated data. The underlying input data to create the aggregation may contain pseudonymous identifiers for example, DeviceID generated by Microsoft in the course of providing the services to the customer, but those identifiers are not used for business operations other than for the sole purpose of creating aggregated data sets that do not themselves contain personal data.

Nor would Microsoft want or need individual-level data for business operations purposes. Thus, for business operations purposes, Microsoft further reduces the privacy risk by aggregating the pseudonymous data so that it no longer contains any individual-level entries and has been combined with data of enough data subjects that individual-level attributes are no longer identifiable. Microsoft then relies solely on the aggregations of this pseudonymized personal data for business operations processing. [...]

This processing involves aggregating information at a product and tenant level, excluding any information about individual users."[260]

149. The EDPS therefore understands that the **user level logs** used to create the statistics in question contain non-pseudonymised and pseudonymised personal data of users.[261] This is because those data reflect information on the use of the Microsoft 365 services by each individual user, and therefore relate to natural persons by reasons of their content.[262] As noted by the EDPS in paragraph 77, such logging may enable tracking the

[260] Reply by Microsoft Ireland of 26 May 2023, Annex 4, p. 5, second, third and fourth paras., p. 10, third para., p. 11, first para., p. 22, second para.

[261] See paras. 43, 45, 47, 49, 51, 52, 77, 109 and 148 of this decision for examples of information that user level logs contain. According to Microsoft Ireland, some logs, e.g. in message tracing in Exchange Online, at the time of creation contain information, e.g. "user principal names", that directly identify the applicable users (reply by Microsoft Ireland of 26 May 2023, Annex 3, pp. 4 and 5, and Annex 6, p. 4). The EDPS understands that these logs may therefore contain also non-pseudonymous personal data. The Commission also e.g. states in its record of processing activities in EC M365 environment that "*service generated data (SGD) contains information related to the data subjects' usage of online services, most notably the user IP address, creation time, site URL and user email address.*" (https://ec.europa.eu/dpo-register/detail/DPR-EC-04966.4, Section 3, para. 4). The pseudonymous data in user level logs also includes end-user identifiers, such as User GUIDs, PUIDs, or SIDs, Session IDs, which when combined with other information, such as a mapping table, identify the end user. See, in this respect, also the Commission's 2021 DPIA, section 3.10.2, p. 53 (also reproduced in the reply by Microsoft Ireland of 26 May 2023, para. 165, p. 49).

[262] See paras. 43, 45, 47, 49, 51, 52, 77, 109 and 148 of this decision. E.g. according to Microsoft Ireland, customer event logs record events when customers initiate actions in enterprise cloud services, such as creating, reading, updating or deleting data or creating, committing or rolling back a database (reply by Microsoft Ireland of 26 May 2023, Annex 3, p. 4). "*Microsoft only needs to process Diagnostic Data in pseudonymized form [...] (i.e., the data [...] will only reveal that 'for User 12345678', the Teams app crashed 5 times in 1 day and 30 times the last month)*" (reply by Microsoft Ireland of 26 May 2023, Annex 5, para. 77.b). The Commission also e.g. states in its record of processing activities in EC M365 environment that "*diagnostic data (also known as telemetry data) is related to the data subjects' usage of office client software*" and that "*service generated data (SGD) contains information related to the data subjects' usage of online services [...]. This data is generated by events that are related to user activity in Office 365.*" (https://ec.europa.eu/dpo-register/detail/DPR-EC-04966.4, Section 3, paras. 3 and 4). The EDPS takes note that Annex A to the EC M365 environment privacy statement shows hundreds of events of user activities that result in logs containing personal data (Commission's reply of 25 May 2023, Annex 2).

activity of individual users[263] that are using Microsoft 365 in extreme detail.[264] Those data are also aimed to e.g. assess whether the use by individual user falls within usual activity parameters for that user or presents anomalous activity outside of usual activity parameters for that user, and therefore relate to natural persons by reason of their purpose.[265] Moreover, the EDPS understands that those data are also aimed to e.g. adapt the services to the specific needs of a user by offering tips to the user or take action where the use by a user presents anomalous activity by investigating security incidents or by troubleshooting a user's problems, and therefore relate to users as natural persons by reason of their effect. Given that in the course of at least certain service operations, Microsoft requires identifying and understanding activities undertaken by individual users and therefore identifying a specific individual,[266] the users to which the data included in user level logs relate, as demonstrated above, are directly or indirectly identifiable. In addition, user level logs allow for the creation of individual level statistics. It follows that the user level logs that are used to create statistics, and are therefore the underlying data prior to pseudonymisation and aggregation that results in statistics, constitute personal data within the meaning of Article 3(1) of the Regulation.

---

[263] The users concerned include not only all Commission's staff, but also staff of other EU institutions or bodies and other individuals, which e.g. cooperate with the Commission using the Commission's tools based on Microsoft 365.

[264] This is supported by the Commission's privacy statement which states that: "*Event data will allow to monitor all activity in the cloud environment of each user.*" (Section 4, point 4 in "EC M365 environment privacy statement.pdf" included in the record, https://ec.europa.eu/dpo-register/detail/DPR-EC-04966.4, Section 7).

[265] See paras. 43, 45, 47, 49, 51, 52, 77, 109 and 148 of this decision. E.g. according to the reply by Microsoft Ireland of 26 May 2023, the exchanges of client/server traffic recorded in customer requests and server traffic logs "*must be logged for security purposes*"; they are also used to "[help] *Microsoft monitor the real-time experience our customers are having*", "*to reconstruct sequences of events and determine their outcome*" and "*to identify or investigate incidents and to monitor application usage for compliance and auditing purposes*" (Annex 3, p. 4). *"One type of activity that is captured in audit logs is user authentication. […] Examples of such activity include successful and failed authentication attempts, account changes (e.g., account creation and deletion, account privilege assignment), and use of privileges. In addition to identifying security events such as brute force password guessing and escalation of privileges, logs can be used to identify who used an application and when it was used. Logs are also useful for security monitoring and response, for example by providing visibility into repeated failed authentication attempts, impossible concurrent uses of the same credentials, or other similar patterns.*" (Annex 3, p. 3). "*Microsoft also relies on Diagnostic Data to detect technical issues – for instance it keeps a record of how many times the Teams app crashed for the User, and compares this against other statistical and performance related metrics received. This allows Microsoft to establish the causes of why the Teams app crashed for that User, and allows it to resolve the issue*" (Annex 5, para. 77.b).

[266] See, in this respect, paras. 131, 157 and 158 of this decision. See also reply by Microsoft Ireland of 26 May 2023: "*Most often, monitoring systems that interact with logs are seeking to identify issues and their scope, and the number of affected users or affected customers can be an object of analysis, but there is no advantage or utility to Microsoft in identifying specific users or customers during routine system operations.*" (Annex 3, p. 2) "*Examples of service operations that can require identifying a specific individual include security monitoring or incident investigations that require identifying and understanding activities undertaken by individual users – however the identification of a specific entity or person during such operations is often only an incidental outcome of the investigative activity. A specific person may also need to be identified from logs to respond to a customer-reported issue (i.e., through a technical support engagement where access to re-identified logs is necessary to resolve an issue for the user(s) reported by customer to be experiencing an issue). Customer self-service logging features may also require that specific users be identified to fulfill customer requirements.*" (Annex 3, pp. 4 and 5) "*Further, as is the case for Diagnostic Data, the purposes for which System-Generated Logs are processed, generally do not require that Microsoft is able to identify the individual user whose data may be reflected in the logs – in turn, Microsoft processes this data in pseudonymized form (using a variety of pseudonymization techniques […]).*" (Annex 5, para. 79). See similarly also reply by Microsoft Ireland of 26 May 2023, Annex 6, pp. 4 and 5.

"Statistics related to Customer Data or Professional Services Data"[267]

150. With regard to point ii) quoted in paragraph 135 of this decision, Microsoft Ireland has stated at the hearing of 23 October 2023 that:

> "*Statistics are aggregated data and do not contain any personal data and were not calculated on the basis of personal data. Therefore, it is impossible to reverse engineer the statistical data to an individual end user, even when one could gain access to the source data on the basis of which these statistics are calculated. For the avoidance of doubt, Microsoft confirms that there are no customer data in these statistics either. Microsoft has referred to the calculation of statistics related to customer data because the statistics are based on metrics which related to customer data. [...] These metrics are generated without the need to process customer data itself. Most of those metrics contain technical system metadata. [...] For example, they relate to storage capacity [...] used by customer data. The metrics or statistics calculated do not consist of, contain, and are not derived from customer data. [...] This is statistical data that does not relate to any individual end-user. It often relates to regions, because we have to scale for regions, or at most a specific tenancy.*"[268]

The Commission has stated at the hearing that: "*statistics are compiled from numerical metrics or measurements relating to the usage of the service, such as how much volume of data is stored on a server or how many users are active in a tenant; the tenant being an instance of the Microsoft 365 service for a particular customer, in [this] case the European Commission*".[269]

151. Similarly, in its reply to the preliminary assessment, Microsoft Ireland states that:

> "*Business operations 'use' of Customer Data is limited to generating statistics, such as measuring the volume of Customer Data stored on servers in a data center as part of planning for required capacity expansion, without acting on what is contained within Customer Data in any cognitively relevant way.*[270] [The] *output that is used for business operations processing is limited to aggregated or statistical data that does not identify or single out individuals and does not contain personal data.*" [271]
> "*Customer Data could be 'processed' for business operations by measuring the Customer Data to create numerical, non-personal data statistics, without accessing or analyzing the content of that Customer Data. For example, the statistics could reflect file size for a service that is billed based on capacity.*"[272]

The EDPS understands that Microsoft aggregates metrics in line with the ISO/IEC 19944[273] (same as for pseudonymised user level logs).

152. Microsoft Ireland gives a further example of statistics generated from metrics as "*when a **User** chats and speaks with colleagues through Teams, Microsoft may create certain*

---

[267] See point ii) quoted in para. 135 of this decision. The EDPS understands that this in essence corresponds to the amendment of 19 December 2023 quoted in para. 124, point ii), of this decision.
[268] Statement by Microsoft Ireland at the hearing of 23 October 2023.
[269] Statement by the Commission at the hearing of 23 October 2023.
[270] Reply by Microsoft Ireland of 26 May 2023, Annex 4, p. 10, second para.
[271] Reply by Microsoft Ireland of 26 May 2023, Annex 4, p. 10, fourth para.
[272] Reply by Microsoft Ireland of 26 May 2023, Annex 5, para. 88, as well as similarly para. 70.
[273] See, in this respect, reply by Microsoft Ireland of 26 May 2023, para. 56 and footnote 101 on p. 53, and Annex 4, p. 12.

overviews (which are 'Aggregated Business Operations Output Data') to measure how many users, or how much volume of data, are relying on a specific Microsoft server – to analyze and measure capacity expansion for certain data centres, to make sure that a given data centre does not get overwhelmed and the ***user*** *does not suffer any interruptions or outages in the service.*" (emphasis added)[274]

153. The EDPS therefore understands that the **metrics** used to create the statistics in question, which may be at the level of specific tenancy (such as the Commission's), relate to customer data, for example to the storage capacity used by customer data. The EDPS also takes note that, according to Microsoft Ireland, the metrics or statistics do not consist of, contain, or are derived from customer data or from other personal data. However, the EDPS considers that metrics related to e.g. storage capacity used by individual users for storing their customer data inherently relate, by reason of their content, to those individuals. This is because the storage capacity to which the metrics relate directly depends on the amount of customer data that the individuals choose to provide through their use of the services. Moreover, Microsoft is able to identify, at least indirectly, such individuals in view of the additional information that it possesses, and in particular logs that contain (pseudonymous) information on the use of the services by each individual user.[275] It follows that the metrics that are used to create statistics, and are therefore the underlying data prior to aggregation that results in statistics, constitute personal data within the meaning of Article 3(1) of the Regulation.

Possibility for Microsoft to reverse pseudonymisation and aggregation

154. The EDPS has asked Microsoft Ireland at the hearing of 23 October 2023 to clarify its previous statements, and in particular how Microsoft ensures "*that each user data* [...] *is uniquely collected*", "*what unique identifier is used, if any, when collecting these source records to be used then for aggregated statistics"* and whether Microsoft keeps *"a correspondence table between the original logs, records, and their corresponding pseudonyms* [...] *and if not,* [...] *[whether]* [Microsoft] *delete[s] the original data, and when* [it is deleted] *in the process"*.[276]

155. At the hearing of 23 October 2023, Microsoft Ireland provided the following reply at the hearing as regards metrics:[277]

> "*Metrics are generated primarily by the operating system [...] to keep [...] infrastructure level statistics. So they are not to the level of users or the use of services, they are to the level of the operating system, which is the underlying system that manages and performs the infrastructure tasks that are there. [...] So there is no data that could even be collected there at that level to a specific user of the service, because those logs, that is a different type of logs, which [were] explained during the second scenario, those are user level."*[278]

[274] Reply by Microsoft Ireland of 26 May 2023, Annex 5, para. 89.

[275] See paras. 43, 45, 47, 49, 51, 52, 77, 109, 148 and 149 of this decision for examples of information that user level logs contain. Metrics might also allow for the creation of individual level statistics.

[276] Question by the EDPS to Microsoft Ireland at the hearing of 23 October 2023.

[277] The EDPS understands that by this statement Microsoft Ireland provides a reply with regard to point ii) quoted in paragraph 135 of this decision (concerning "statistics related to Customer Data or Professional Services Data").

[278] Statement by Microsoft Ireland at the hearing of 23 October 2023.

156. Microsoft Ireland provided the following reply at the hearing as regards user level logs,[279] for which it clarified that Microsoft uses "*two main mechanisms*":

> *"The first mechanism is for a user ID which ends up in a log. That user ID never relates to the actual name, first name, directly identifiable information. We use that pseudonymous identifier that is created as soon as the user is registered into the directory, the Azure Active Directory or Entra ID directory that was explained. So that pseudonymous identifier is used directly in the logs. The mapping table therefore is also contained in Azure Active Directory. Azure Active Directory contains the user identifier, the pseudonymous identifier mapped to the user details itself. When the logs are created, the logs directly use that pseudonym identifier. [...] It gets the object ID. So at the source, that part is pseudonymized from the start. So there is no source copy that has a copy of that same log with the directly identifiable identifier. [...] If we use the user ID [in logs], [...] we use the already pseudonymized identifier in Azure Active Directory [- the ObjectID]. So that's not rehashed. So the hash mechanism that the scrubber uses, the scrubbing service, that's for the remaining personal data in any logs. So any log from the start uses that ObjectID from Azure Active Directory, which is already a pseudonymized identifier.*
>
> *The second part [...] is about the IP address, for example, [and] other personal data [e.g. MAC address of user's device] that may end up in a log, which is then pseudonymised by the scrubber. If the scrubber takes the source data, then performs its HMAC functioning, that's where the HMAC mechanism comes into place. It transforms the log [...], so it [doesn't] keep the source. So if we would have to re-identify, we should have to recreate the whole log again, so the source is not kept. [...] [H]ashing is an HMAC mechanism that we use. HMAC-256 is a one-way hash. So what goes in, the outcome cannot be reversed back from that hash itself. And it's a one-way cryptographically secure hash mechanism that we use, which is the example here. [...] There is no linking table nor source data that relates in a fixed table the user identifier in Azure Active Directory with any of the other fields. [...] Any of the other fields typically are dynamic fields and IP address may change over time for a user, MAC addresses may change. So there's no table that links those two together. Most logs [don't] contain the user ID because for this purpose it's not necessary. Everything we do always needs that purpose. So this log only contains the pseudonymized hashes of the IP address and the MAC addresses and no user object identifier. Therefore, this could not be related through even the table that we do maintain in Azure Active Directory between the user object and the username."*[280]

157. In its reply to the preliminary assessment, Microsoft Ireland has provided a "*chart* [with] *an overview of the obligations on and nature of* [...] *System-Generated Logs of user activity in online service*", stating in particular:

> *"Log records that hold any personal data directly attributable to an individual provided to Microsoft through use of the online services. Benefit from the following protections: [...]*
> *• The personal data must be provided to customer when the customer instructs us to provide it in response to a data subject request. Service features support this requirement.*

[279] The EDPS understands that by this statement Microsoft Ireland provides a reply with regard to point i) quoted in paragraph 135 of this decision (concerning "aggregated statistical, non-personal data from data containing pseudonymized identifiers").

[280] Statement by Microsoft Ireland at the hearing of 23 October 2023.

This [...] includes:
- Look up tables to resolve pseudonyms in System-generated Logs where they still contain the identifiable personal data or Customer Data in plaintext
- Identity of users to resolve globally unique pseudonyms
- If encryption is used to de-identify plain text to make it suitable for use as a cypher pseudonym in system generated data, then the key-secret for decryption must be handled as for Customer Data

Log records that hold only pseudonymized personal data that is not directly attributable to an identified individual benefit from the following protections: [...]
• The pseudonymized personal data must be provided to customer in case of a data subject request reporting instruction from customer, which requires re-establishing the connection with an identifiable individual to fulfill the customer's instruction.
This [...] only [includes]
- Service log records that contain personal data that has been pseudonymized."[281]

The EDPS therefore understands that for pseudonymised personal data, regardless of whether they are or are not directly attributable to an identified individual, Microsoft retains:

a) look-up tables to resolve pseudonyms in system-generated logs,
b) the identity of users to resolve globally unique pseudonyms,
c) key-secrets for decryption of cypher pseudonyms in system generated data that had been encrypted to de-identify plain text, and
d) other additional information that enables Microsoft to resolve pseudonymised data and re-establish the connection with an identifiable individual (underlying non-pseudonymised and pseudonymised personal data[282]).

158. In its reply to the preliminary assessment, Microsoft Ireland also states that:

"Diagnostic Data is processed by Microsoft in pseudonymized form. Microsoft carries out pseudonymization by removing direct identifiers from the data (e.g. name, e-mail) and replacing them with unique numeric codes.[283] *[...] Diagnostic Data is pseudonymized as Microsoft has no interest or purpose for identifying individuals in the context of Diagnostic Data.*[284] *[...] While some System-Generated Logs can contain non-pseudonymized personal identifiers when they are generated within the services located in the EU, these logs are then pseudonymized before transfer to long-term storage and are subsequently used in pseudonymized form. The limited exceptions are if a specific operational scenario, such as identifying a bad actor as the outcome of a security investigation, or assisting the customer with a customer-initiated support interaction related to an identified user, requires re-identifying a user from the pseudonymized logs. Service-Generated Data used for business operations is always processed by Microsoft in aggregated form. Microsoft carries out pseudonymization by removing direct identifiers from the data (e.g. name, e-mail) and replacing them with unique numeric codes.* [285] *[...] System-Generated Logs are processed in pseudonymized form as Microsoft has no interest or purpose for*

[281] Reply by Microsoft Ireland of 26 May 2023, Annex 4, p. 6.
[282] See, in this respect, paras. 131 and 141.
[283] Reply by Microsoft Ireland of 26 May 2023, Annex 5, para. 117.
[284] Reply by Microsoft Ireland of 26 May 2023, Annex 5, para. 121.
[285] Reply by Microsoft Ireland of 26 May 2023, Annex 5, para. 123.

reidentifying individuals; [...] Service-Generated Data are aggregated when used for business operations so that they do not link to any individual user. [286]"

159. As regards **access to the content** of customer data or professional service data and re-identification (including by singling out) of individuals by people involved in business operations, the Microsoft Ireland also states in its reply to the preliminary assessment that:

"*Business operations processing is not applied to all Customer Data. Specifically, in no case does Microsoft permit access to or analysis of the content of Customer Data for business operations processing.*[287]

Consistent with its practices around all business operations, Microsoft does not permit [people working on billing or account management / people involved in calculating or receiving compensation / people involved in internal reporting or modelling / people involved with financial reporting] as part of this business operation to: (a) see usage by individuals or to re-identify individuals from the pseudonymous identifiers; or (b) access the content of Customer Data, including personal data within the content of Customer Data or Professional Services Data.[288]

While the aggregated data is non-personal and does not permit singling out individuals, it would not, for example, be possible to use anonymous data to develop the aggregations since this would not allow reaching the business operations purposes."[289]

160. The amendment of 19 December 2023 also regulates processing of the content of the customer data, of the functional data and of the professional services data. Under the amendment, access to the content of customer data and of professional services data is not permitted.[290] However, as regards functional data, access to, as well as analysis of, its content is excluded only with regard to calculation of non-personal numerical statistics and not with regard to the calculation of aggregated non-personal numerical statistics from data containing pseudonymised identifiers.[291] At the hearing of 23 October 2023, after having submitted in its reply to the preliminary assessment an amendment proposal that is in this regard essentially equivalent to the amendment of 19 December 2023, Microsoft Ireland has stated that:

"[it] *would like to reiterate that it does not process any content found in customer data or other data* categories *collected under the ILA 2021 for business operations. Microsoft does not need to because the actual content is irrelevant to its business*

[286] Reply by Microsoft Ireland of 26 May 2023, Annex 5, para. 125.
[287] Reply by Microsoft Ireland of 26 May 2023, Annex 4, p. 10, second para., and similarly p. 21, first para., p. 22, first para, p. 23, second para, p. 24, first para.
[288] Reply by Microsoft Ireland of 26 May 2023, Annex 4, p. 13, last para., p. 14, second and last paras., p. 15, second para.
[289] Reply by Microsoft Ireland of 26 May 2023, Annex 4, p. 18, second column.
[290] Commission's email of 19 December 2023, Annex 2 (Amendment to Contract Documents), p. 2, second para., and p. 5, last para. Already prior to that amendment, access to the content of customer data was not permitted for business operations purposes (2021 ILA, p. 29). Prior to that amendment, such prohibition was not in place neither for professional services data nor functional data.
[291] Commission's email of 19 December 2023, Annex 2 (Amendment to Contract Documents), pp. 2 and 5.

operations for which it needs [...] metrics related to the use and operation of its services".[292]

However, as explained, this statement is not supported contractually as regards functional data. In view of the amendment of 19 December 2023, the EDPS cannot consider that access to the content of functional data is not permitted for Microsoft's business operations purposes.

161. The EDPS notes another discrepancy between the contractual provisions of the applicable 2021 ILA and the stated processing. In its reply to the preliminary assessment, Microsoft Ireland has stated, by using the present tense, that the White Paper on Business Operations explains that "*Microsoft **uses** pseudonymized, aggregated data as input for four types of processing for Business Operations*" (emphasis added).[293] At the time, no amendment was concluded modifying the number of business operations purposes from six to four. Moreover, referring to the content of the amendment proposal, Microsoft Ireland has stated that: "*This is something that is not yet finalised in the contract, but what the contract would be doing would be applying what we're already doing in practice*".[294] The EDPS therefore understands that the content of the amendment had been applied in practice, without any corresponding contractual modifications to the 2021 ILA.

162. The EDPS considers that on the basis of Microsoft's written and oral submissions made in reply to the preliminary assessment,[295] it has not been demonstrated that the data having undergone pseudonymisation and aggregation (for user level logs) or solely aggregation (for metrics) for use in Microsoft's business operations are effectively anonymised, i.e. no longer considered personal data within the meaning of the Regulation.

[292] See similarly reply by Microsoft Ireland of 26 May 2023, Annex 4, p. 10, second para., and p. 13, last para.
[293] Reply by Microsoft Ireland of 26 May 2023, para. 8.
[294] Statement by Microsoft Ireland at the hearing of 23 October 2023.
[295] See in this respect paras. 131 and 135 to 160 of this decision.

163. The EDPS concludes that Microsoft reasonably has at its disposal means enabling it to link the data to those users and thereby to identify those persons with the help of additional information that it retains, for the reasons set out below.[296] [297]

164. **First**, both the non-pseudonymised and pseudonymised personal data[298] relating to individuals are retained after the aggregation and are otherwise processed either for the purpose of providing online services or for compliance with legal obligations,[299] including in response to data subject requests.[300] Microsoft also retains look-up tables, identity of users and other information which enable it to identify the natural persons using its services by resolving the pseudonyms.[301] Moreover, Microsoft retains the secret keys to decrypt pseudonyms in system generated data, which also enable it to identify the natural persons using its services.[302] All of these are information in Microsoft's possession which Microsoft can use to identify an individual.[303] [304] Which Microsoft entity retains this additional information is immaterial, since it is not required that all

---

[296] The EDPS points out that in addition to Microsoft, also the Commission retains additional information which can be used to link the data concerned in processing for Microsoft's business operations to natural persons using the Commission's tools based on Microsoft 365 and to identify them. This is, in particular, information relating to the individual user using the Commission's tools based on Microsoft 365 which is relevant for the Commission to approve that individual's use of the Commission's tool, to create a user account for that individual and for authentication when the individual logs into their account in the Commission's tool. See, in this respect, the Commission's 2021 DPIA, section 3.10.2, p. 53 (also reproduced in the reply by Microsoft Ireland of 26 May 2023, para. 165, p. 49). The 2021 DPIA lists various types of personal data under identification data, personal characteristics and professional data that the Commission identified under "*Business process 1: Identity and access management of Office 365 applications*". In particular, under identification data, the DPIA lists: "*- Personal Identifying Information: Name, title, address (private and professional), previous addresses, phone number (private and professional), Identifier; (An identifier has been created by Microsoft and is tied to the user of a Microsoft service. When combined with other information, such as a mapping table, EUPI identifies the end user; examples User GUIDs, PUIDs, or SIDs, Session IDs; EUPI does not contain information uploaded or created by the customer); - Electronic Identifying Information: IP address, cookies, connection data. [...] The following user attributes may be shared in context of Azure AD Connect Sync. DIGIT deselects attributes in order to fulfil data minimisation requirements (i.e. to select only the attributes that are required to facilitate identity and access management for Office365). DIGIT determines per application which attributes are necessary, and which to deselect. Attributes include, for example: - displayName, - samAccountName, - userPrincipalName, - department, - managedBy, - mobile, - postalCode, - streetAddress, - telephoneAssistant*".

[297] In accordance with Article 3(1) and recitals 16 and 18 of the Regulation, as interpreted in light of the case-law of the Court of Justice. See, to that effect, also judgment in Case C-319/22, *Gesamtverband Autoteile-Handel (Accès aux informations sur les véhicules)*, ECLI:EU:C:2023:837, paras. 45 to 50.

[298] See in this respect paras. 131, 141, 142, 148, 149, and 156 to 158, as well as 132 of this decision. The underlying raw data and intermediate pseudonymous data. This data includes end-user identifiers, such as User GUIDs, PUIDs, or SIDs, Session IDs, which when combined with other information, such as a mapping table, identify the end user. See, in this respect, also the Commission's 2021 DPIA, section 3.10.2, p. 53 (also reproduced in the reply by Microsoft Ireland of 26 May 2023, para. 165, p. 49).

[299] See, in this respect, paras. 131, 157 and 158 of this decision.

[300] See, in this respect, para. 157 of this decision.

[301] See, in this respect, paras. 148 and 158 of this decision.

[302] See, in this respect, para. 158 of this decision.

[303] See, in this respect, recital 16 of the Regulation, as well as paras. 127 and 132 of this decision. See, in this respect, also Article 29 Working Party's Opinion 05/2014, p. 29, fifth para.

[304] See, in this respect, also the Commission's 2021 DPIA, section 3.10.2, p. 53 (also reproduced in the reply by Microsoft Ireland of 26 May 2023, para. 165, p. 49). "*Business process 1: Identity and access management of Office 365 applications. [...] An identifier has been created by Microsoft and is tied to the user of a Microsoft service. When combined with other information, such as a mapping table, EUPI identifies the end user. [...] User attributes [that] may be shared in context of Azure AD Connect Sync, [...] include, for example: - displayName, - samAccountName, - userPrincipalName, - department, - managedBy, - mobile, - postalCode, - streetAddress, - telephoneAssistant*". The DPIA also states on p. 33 that "*Azure AD is operated from EU data centres for customers having an EU-based tenant (like EC), so the synced attributes of EC users do not go to the US*".

the information enabling an individual to be identified are in the hands of a single entity.[305] This is all the more immaterial since Microsoft entities form part of the same corporate group and any of the Microsoft entities may re-identify or re-establish the link with an identifiable individual for different reasons (e.g. for fulfilling the customer's instruction, for replying to data subject requests, for complying with legal obligations, for support and for security, as well as for some business purposes such as financial reporting). Thus, this already demonstrates that all Microsoft entities have means reasonably likely to be used to identify the natural persons using Microsoft 365.

165. The EDPS takes note of claims by Microsoft Ireland that any of fields other than the user identifier are typically dynamic fields and that the IP and MAC addresses may change for a user.[306] The EDPS understands that Microsoft Ireland makes this statement to substantiate that reversing pseudonymisation is more difficult. It is true that in the context of big organisation customers' use of Microsoft services, it is likely that IP addresses and MAC addresses of users may change, since a user may be connecting from different places or using different devices to connect. However, that individual user will still have a user account (which contains also a user ID, that Microsoft stores as ObjectID in Azure Active Directory[307]) set up to use those Microsoft services from the enterprise, and diagnostic and service generated data will still be collected when that user uses those Microsoft services.[308] The look-up table retained by Microsoft[309] is the information additional to user Object ID that can be used to identify an individual user, and thus Microsoft has means reasonably likely to be used to identify that user.[310] The EDPS therefore considers that Microsoft could still link that additional information together by using one or more of the three ways to reverse pseudonymisation that are mentioned in Microsoft's reply to the preliminary assessment.[311] In addition, the fact that IP addresses and MAC addresses of users may change does not imply that they do indeed change or change regularly in all cases. In particular, it is not common for EU staff members to change their corporate devices, and thus their MAC address, very frequently.

166. **Second**, whether pseudonymisation and aggregation, when used together[312] or when only aggregation is used,[313] effectively anonymise personal data, also depends on how these techniques and processes are implemented. The EDPS has not received, either from the Commission or Microsoft Ireland, complete information on how the different techniques, in particular **pseudonymisation using HMAC** based on NIST FIPS 198-1 and SHA-256 in accordance with ISO/IEC 10118-3:2016 standard[314] and **aggregation,**

---

[305] See, in this respect, recital 16 of the Regulation, as well as judgment in Case C-319/22, *Gesamtverband Autoteile-Handel (Accès aux informations sur les véhicules)*, ECLI:EU:C:2023:837, para. 45 (and paras. 42 and 43 of the judgment in Case C-582/14, *Breyer*, EU:C:2016:779, cited there).

[306] See, in this respect, para. 156 of this decision.

[307] See, in this respect, para. 156 of this decision.

[308] See also paras. 47, 49, 51, 52, 77, 109 and 148 of this decision.

[309] These are part of the non-pseudonymised and pseudonymised personal data retained by Microsoft after the aggregation. See in this respect 131, 141, 142, 148, 154 and 158, as well as 132 of this decision.

[310] See, in this respect, also para. 164 of this decision.

[311] See paras. 148, 154 and 164 of this decision. Microsoft retains look-up tables to resolve pseudonyms in system-generated logs, identity of users and other information to resolve globally unique pseudonyms, as well as secret keys to decrypt pseudonyms in system generated data.

[312] To create "*aggregated statistical, non-personal data from data containing pseudonymized identifiers*" (from user level logs).

[313] To create "*statistics related to customer data or professional services data*" (from metrics).

[314] See, in this respect, para. 142 of this decision.

reportedly in accordance with ISO/IEC 19944 standard,[315] have been implemented.[316] The EDPS notes that in any event applying the ISO/IEC 19944 series of standards when aggregating pseudonymous personal data does not demonstrate that such aggregation has effectively resulted in their anonymisation.[317] In this regard, the EDPS stresses that the ISO/IEC 19944 series of standards do not provide criteria on how to aggregate data, and in particular so as to reach anonymisation. Neither has the EDPS received complete information as to all possible types of aggregation carried out by Microsoft for its various own business operations.

167. Such information is indispensable for determining whether individuals can still be singled out, inferred or linked given the nature of the data collected. In line with the accountability principle under Article 4(2) as well as under Article 26 of the Regulation, it is for the Commission as the controller for the initial processing to demonstrate that the data further processed for the processor's own business purposes are anonymised, as the processor claims. In particular, it is for the Commission to demonstrate, based on the information obtained from Microsoft Ireland, that the implemented technical and organisational measures, including pseudonymisation and aggregation, when used together,[318] or when only aggregation is used,[319] render the data concerned anonymous. This means demonstrating that singling out, inference or linking of individuals from aggregated data is no longer possible.

168. **Third**, Microsoft claims to maintain strict technical and operational measures regarding re-identification. This includes a prohibition of any attempt to re-identify de-identified

---

[315] See, in this respect, paras. 147 and 148 of this decision.

[316] HMAC implementation would e.g. depend on the following elements:
- whether the encryption and hashing algorithms and their parameterization (e.g., key length, operating mode, if applicable) conform to the state-of-the-art and can be considered robust against cryptanalysis performed by Microsoft or another entity (e.g. the public authorities in the recipient country) taking into account the resources and technical capabilities (e.g., computing power for brute-force attacks) available to them,
- whether the strength of the encryption, hashing and key length takes into account the specific time period during which the confidentiality of the encrypted hashed personal data must be preserved,
- whether the encryption and hashing algorithms are implemented correctly and by properly maintained software without known vulnerabilities the conformity of which to the specification of the algorithm chosen has been verified, e.g., by certification,
- whether the keys are reliably managed (generated, administered, stored, if relevant, linked to the identity of an intended recipient, and revoked).

See, by analogy, conditions 2 to 5 of use case 1 of EDPB Recommendations 1/2020 on supplementary measures.

[317] ISO/IEC 19944 series of standards provides description of data flows, data categories (including description of pseudonymised, anonymised and aggregated data) and data use categories, as well as guidance on how to describe them to stakeholders. ISO/IEC 19944 series of standards **cannot be used for compliance directly**. Instead, it provides a set of concepts and definitions that can be used for transparency about how data are used in an ecosystem of devices and cloud services. It also aims to improve the understanding of the data flows that take place in an ecosystem consisting of devices accessing cloud services. ISO/IEC 19944 series of standards **does not provide standards on how to carry out pseudonymisation, anonymisation and aggregation** of data captured, processed, used and shared in cloud services. ISO/IEC 19944-1:2020 standard, e.g. provides a definition of "data aggregation" in section 9.2.3, and a statement in section 8.4.3 on processes that are "not subject to the original legal constraints, such as anonymisation or aggregation of data" but does not provide how to aggregate data so as to reach anonymisation. Section 9.2.9 of ISO/IEC 19944-1:2020 standard is on "data re-identification", however it does not contain any demonstration of effective anonymisation through aggregation either.

[318] To create "*aggregated statistical, non-personal data from data containing pseudonymized identifiers*" (from user level logs).

[319] To create "*statistics related to customer data or professional services data*" (from metrics).

data[320] and to carry out individual-level statistics on the basis of such de-identified data by its staff performing business operations.[321] It also includes ensuring that "*access to token look-up tables"* and handling of *"key-secret for decryption"* are the same as the access and handling applying to customer data.[322] In the EDPS' view, the fact that Microsoft Ireland deems such measures necessary is an indication that Microsoft Ireland does not consider that the data can no longer be used to identify a natural person by any means reasonably likely to be used, such as singling out. Where a certain processing operation is technically not feasible, there is no need to prohibit it by way of internal rules, including any intra-group corporate rules. Indeed, such measures do not lead to the conclusion that it is not technically feasible for those staff to get such individual statistics or access to non-pseudonymised and pseudonymised data (i.e. raw data) if Microsoft changes its internal policies or is required to do so e.g. by law or by a public authority.[323]

169. The EDPS has not received submissions by the Commission and Microsoft Ireland that allege or demonstrate that contractual commitments imposing a prohibition of re-identification have been made between entities wholly owned, directly or indirectly, by Microsoft Corporation. However, the EDPS considers that in any event a parent-subsidiary relationship might render such contractual commitments insufficient to exclude that means reasonably likely to be used to re-identify individuals still exist in the hands of the parent company or of the subsidiary.

170. Microsoft claims that it does not want or need to process individual-level data for business operations. The EDPS considers that this is irrelevant in ascertaining whether Microsoft or any other entity has means reasonably likely to be used, such as singling out, to identify a natural person directly or indirectly. Microsoft may decide, out of preference or necessity, to process individual-level data for business operations.

171. The EDPS considers that, in principle, it is not necessary for the EDPS to re-demonstrate that the data are personal where such data were,[324] either undisputedly personal data and/or were demonstrated to be personal data,[325] and for which, following pseudonymisation and aggregation,[326] or only aggregation,[327] it has been demonstrated that Microsoft has means reasonably likely to be used to identify the natural persons concerned directly or indirectly. Such data (user level logs and metrics), before pseudonymisation and/or aggregation, relate to identifiable natural persons, as demonstrated in paragraphs 149 and 153.

---

[320] Following pseudonymisation and aggregation data for "*aggregated statistical, non-personal data from data containing pseudonymized identifiers*" (from user level logs) or following aggregation for "*statistics related to customer data or professional services data*" (from metrics), as argued by Microsoft Ireland.

[321] Microsoft's letter to the Commission of 15 April 2020, p. 4. Similarly, reply by Microsoft Ireland of 26 May 2023, Annex 4, p. 5, second para, and p. 13, last para. See, in this respect, also para. 159 of this decision.

[322] Reply by Microsoft Ireland of 26 May 2023, Annex 4, p. 5, fourth para, and p. 6. See, in this respect, also paras. 148 and 157 of this decision.

[323] See, in this respect, EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, paras. 109 and 110.

[324] Prior to pseudonymisation and aggregation (user level logs) or aggregation (metrics).

[325] See paras. 27, 43, 47, 49, 51, 52 77, 109, 148, 149 and 153 of this decision.

[326] To create "*aggregated statistical, non-personal data from data containing pseudonymized identifiers*" (from user level logs).

[327] To create "*statistics related to customer data or professional services data*" (from metrics).

172. Nonetheless, out of excess of caution, the data that Microsoft has pseudonymised and aggregated,[328] or only aggregated,[329] relate to natural persons, by reason of their content, because the content of the aggregated data created from user level logs or metrics reflects the specific use by natural persons who are the users of the Commission's tools based on Microsoft 365.[330] Moreover, such aggregated data relate to natural persons also by reason of their purpose, because the stated aim of such data is e.g. to ensure that the user as a natural person does not suffer any interruptions or outages in the service[331] or to understand whether users are activating and getting value from purchased products.[332]

173. It follows from the EDPS' assessment in paragraphs 127 to 172 that data that have undergone pseudonymisation and aggregation (for user level logs) or only aggregation (for metrics)[333] in order to be further processed for Microsoft's business operations, relate to natural persons and that Microsoft has the means reasonably likely to be used to identify those natural persons directly or indirectly.[334] The EDPS therefore concludes that such data are not anonymised and therefore remain personal data within the meaning of Article 3(1) of the Regulation.[335]

Assessment of controllership

174. Under Article 3(8) of the Regulation, a controller is the EU institution or body which, alone or jointly with others, determines the purposes and means of the processing of personal data.[336] It follows that the controller must determine both purposes and (essential) means of the processing.[337] Essential means are means closely linked to the purpose and the scope of the processing, such as the types of personal data processed, the duration of the processing, the categories of recipients and of data subjects. The Court of Justice has held that a natural or legal person who exerts influence over the processing of personal data, for their own purposes, and who participates, as a result, in

---

[328] To create "*aggregated statistical, non-personal data from data containing pseudonymized identifiers*" (from user level logs).

[329] To create "*statistics related to customer data or professional services data*" (from metrics).

[330] In its reply to the preliminary assessment, Microsoft Ireland gives the following example of statistics (without distinction whether they were created user level logs or metrics) used for compensation of Microsoft's staff and business partners: *"[...] the data processing employed to develop usage-based compensation may involve* ***counting the number of users who have sent at least one email*** *in a month (without identifying the users themselves), a metric that is used to understand whether users are activating and getting value from purchased products.*" (reply by Microsoft Ireland of 26 May 2023, Annex 4, p. 22, second para.). As regards statistics obtained from metrics (statistics related to customer data or professional services data), see also paras. 152 and 153 of this decision, which show that the statistics are created when individual users use the services and reflect such use, including how many users are relying on a specific Microsoft server.

[331] Reply by Microsoft Ireland of 26 May 2023, Annex 5, para. 89. See also para. 152 of this decision.

[332] Reply by Microsoft Ireland of 26 May 2023, Annex 4, p. 22, second para.

[333] I.e. statistics created from user level logs or metrics.

[334] See in this respect recital 16 of the Regulation, as well as paras. 127 and 132 of this decision. See, to that effect, also judgment in Case C-319/22, *Gesamtverband Autoteile-Handel (Accès aux informations sur les véhicules)*, ECLI:EU:C:2023:837, paras. 45, 46 and 49, and the case-law cited there.

[335] In accordance with Article 3(1) and recitals 16 and 18 of the Regulation, as interpreted by the case-law of the Court of Justice. See, to that effect, also judgment in Case C-319/22, *Gesamtverband Autoteile-Handel (Accès aux informations sur les véhicules)*, ECLI:EU:C:2023:837, paras. 45 to 50.

[336] See also para. 113 of this decision.

[337] See also EDPB Guidelines 07/2020, para. 36.

the determination of the purposes and means of that processing, may be regarded as a controller.[338]

175. Prior to the amendment of 19 December 2023, the DPA granted Microsoft Ireland the right to process data for the purpose of "*business operations*", which were defined to cover the following six purposes ('business purposes'):[339]

    a) billing and account management;
    b) compensation (e.g. calculating employee commissions and partner incentives);
    c) internal reporting and business modelling (e.g. forecasting, revenue, capacity planning, product strategy);
    d) combatting fraud, cybercrime and cyberattacks;
    e) improving the core functionality of accessibility, privacy or energy efficiency; and
    f) financial reporting and compliance with legal obligations.

176. The DPA has provided, both prior to the amendment of 19 December 2023 and following that amendment, that Microsoft is to process personal data for its business purposes "*on behalf of the Customer*",[340] which implies that Microsoft is to carry out such processing as a processor.[341] The Commission has confirmed this view, stating that "*Microsoft has agreed to process personal data for the six business operations [...] as a processor*".[342] Moreover, following that amendment, the DPA provides that the "*Customer instructs Microsoft*" to carry out processing for the purpose of Microsoft's business operations.[343] The EDPS understands that this further underlines that the DPA designates Microsoft as the processor with regard to processing for its own business purposes.

177. On 19 December 2023, the Commission and Microsoft Ireland concluded an amendment to the DPA. Following that amendment, Microsoft's business operations consist of the following purposes:

    a) billing and account management;
    b) compensation (e.g. calculating employee commissions and partner incentives);
    c) internal reporting and business modelling (e.g. forecasting, revenue, capacity planning, product strategy);
    d) financial reporting.[344]

---

[338] See, to that effect, judgment in Case C-25/17, *Jehovan todistajat*, EU:C:2018:551, para. 68, judgment in Case C-807/21, *Deutsche Wohnen*, ECLI:EU:C:2023:950, para. 41, and judgment in Case C-683/21, *Nacionalinis visuomenės sveikatos centras*, ECLI:EU:C:2023:949, para. 30.

[339] Section on "*Processing for Microsoft's Business Operations*" in the main body of the DPA, 2021 ILA, p. 29.

[340] Section on "Nature of Data Processing; Ownership" in the main body of the DPA, 2021 ILA, p. 28.

[341] See the definition of "*processor*" in Article 3(12) of the Regulation.

[342] Commission's substantive reply of 15 October 2021, para. 2.3.2.5, p. 8. While this statement dates from 2021, the Commission has not subsequently made a statement to the contrary. With regard to the amendment to the DPA of 19 December 2023 which modifies the number of business operations purposes, the Commission stated in its email of the same date that the "*changes do not introduce new or fundamentally different processing operations and therefore, by [its] understanding, no new facts to the investigation*". The EDPS therefore considers the quoted statement of 2021 with regard to controllership related to Microsoft's business purposes as maintained by the Commission.

[343] Commission's email of 19 December 2023, Annex 2 (Amendment to Contract Documents), pp. 2, 4 and 5.

[344] Commission's email of 19 December 2023, Annex 2 (Amendment to Contract Documents), pp. 1 and 2, point 2; see also in this regard similar amendments for software and professional services, respectively, on pp. 4 and 5, point 7, and pp. 5 and 6, point 9.

178. The EDPS understands, based on the amendment to the DPA of 19 December 2023 as noted in paragraph 177 of this decision, that the following purposes are no longer included among Microsoft's business operations purposes:

a) improving the core functionality of accessibility, privacy or energy efficiency,
b) combatting fraud, cybercrime and cyberattacks, and
c) compliance with legal obligations.[345]

179. However, this does not mean that Microsoft Ireland is no longer permitted to process personal data for these three purposes at all, at least to the extent that they fall under the provision of the services. The EDPS considers that the DPA, both prior and after the conclusion of the amendment of 19 December 2023,[346] implicitly includes these three purposes within the description of the "*Processing to Provide Customer the Online Service*".[347] In particular, under the part of that description that reads that "'*to provide' an Online Service consists of [...] processing data as necessary to [...] otherwise comply with law*". Moreover, 'financial reporting' as one of the four remaining business operations purposes also entails complying with the "*applicable laws and regulations*", as stated by Microsoft Ireland.[348]

180. The EDPS acknowledges that Article 29(3)(a) of the Regulation allows a processor to deviate from instructions from the controller if required to do so by EU or Member State law to which the processor is subject. However, in such a case, the EDPS considers that such a processor is acting as a controller in respect of that processing.

181. This view is consistent with the EDPB's statement that:

> "c*ommonly, [...] the law will establish a task or impose a duty on someone to collect and process certain data. In those cases, the purpose of the processing is often determined by the law. The controller will normally be the one designated by law for the realization of this purpose, this public task.*"[349]

182. It is also consistent with the case-law of the Court of Justice, according to which a body responsible for the processing of the personal data in accordance with the purposes and means prescribed by law is to be considered a controller under the Regulation.[350] It can therefore generally be presumed that an entity that carries out processing required by law is acting as a controller.[351] The EDPS therefore considers that when Microsoft

---

345 Commission's email of 19 December 2023, Annex 2 (Amendment to Contract Documents), p. 1, point 2.

346 See para. 86 of this decision for how the 2021 ILA prior to the amendment of 19 December 2023 defines providing an online and professional service. The amendment of 19 December 2023 has modified the description of "to provide" an online service only by stipulating that "ongoing improvement" is limited to the online service that the customer uses or subscribes to.

347 2021 ILA, pp. 28 and 29, and Commission's email of 19 December 2023, Annex 2 (Amendment to Contract Documents),

348 Reply by Microsoft Ireland of 26 May 2023, Annex 4, p. 15.

349 EDPB Guidelines 07/2020, para. 24.

350 C-231/22, Belgian State, ECLI:EU:C:2024:7, para. 35.

351 The EDPS does not take a position on whether processing for which Microsoft acts as a controller complies with the GDPR, which is for the competent supervisory authorities in Member States to determine, taking into account also EDPS' findings (see, to that effect, case-law of the Court of Justice in Case C-645/19 (*Facebook Ireland and Others*) and in Case C-252/21 (*Meta Platforms and Others (Conditions générales d'utilisation d'un réseau social)*).

processes data to comply with its legal obligations, it is acting as a controller under the GDPR.

183. Even though the DPA no longer lists 'complying with legal obligations'[352] as one of Microsoft's business operations purposes, it still contains that purpose, with Microsoft Ireland as the processor, within the provision of services to the Commission. In view of the above, the EDPS recommends that the contract between the Commission and Microsoft Ireland clarify that Microsoft Ireland acts as a controller when it complies with its legal obligations. When Microsoft processes personal data in order to comply with its legal obligations, such processing cannot be considered as effectively falling within the provision of online services and is not carried out on the Commission's behalf.

184. To state that a processor processes personal data on behalf of the controller signifies that it is serving the controller's interests in carrying out a specific task and is following the controller's documented instructions, at least with regard to the purpose and essential means of the processing.[353]

185. The legal status of an actor as either a controller or processor cannot, in principle, be determined only by a formal designation in a contract.[354] It depends on the factual circumstances of the processing.[355] The controller is the one that determines the purposes and essential means of the processing. If an entity involved in the processing does not pursue any purpose(s) of its own in relation to the processing activity, but is merely being paid for services rendered, it is acting as a processor.[356]

186. In its reply to the preliminary assessment, Microsoft Ireland claims that:

> "*The fact that some of the processing happens to also be in Microsoft's interest in providing the services is irrelevant to determine controllership*".[357]

The EDPS considers that such interpretation would be contrary to the settled case-law of the Court of Justice according to which processing of personal data for mutual benefit or in the interests of both parties leads to the conclusion that both parties determine the purposes of the processing.[358] Obtaining a benefit arising from a processing operation or pursuing an interest through a processing operation is an indication of determining the purposes of the relevant processing operation.[359]

---

[352] Including in so far as those legal obligations pertain to combatting fraud, cybercrime and cyberattacks, or to improving accessibility, privacy or energy efficiency.

[353] EDPS Guidelines on the concepts of controller, processor and joint controllership under Regulation (EU) 2018/1725, p. 16. See also EDPB Guidelines 07/2022, paras. 80 and 81.

[354] Distinct from the possibility under Article 3(8) of the Regulation for the controller or the specific criteria for its nomination to be provided for by Union law where the purposes and means of such processing are determined by a specific Union act.

[355] See EDPB Guidelines 07/2020, para. 12.

[356] Cf. EDPB Guidelines 07/2020, paras. 62 and 68. The existence of a mere commercial benefit for the parties involved is not sufficient to qualify as a purpose of processing.

[357] Reply by Microsoft Ireland of 26 May 2023, para. 192.

[358] Case C-40/17, *Fashion ID*, ECLI:EU:2018:1039, para. 80. See also Case C-210/16, *Wirtschaftsakademie*, ECLI:EU:C:2018:388, paras. 34 and 39, from which it follows that there is joint controllership where each entity pursued its own interest but both entities participated in the determination of the purposes and means of the processing of personal data for that processing operation.

[359] Cf. EDPB Guidelines 07/2020, paras. 60 to 62 and pp. 50 and 51.

187. In its reply to the preliminary assessment, Microsoft Ireland also states with regard to processing for its own business purposes that:

> "*The Commission here has determined the essential purposes and means of the processing, and has adequately instructed Microsoft through the 2021 ILA, and the various ad hoc instructions provided over the course of the contractual relationship.*"[360]

In this regard, the EDPS considers that Microsoft Ireland has at least to an extent determined the purposes and essential means of processing carried out for its remaining own business purposes,[361] for the following reasons.

188. As established above, the Commission has not sufficiently determined the types of personal data processed for the provision of services and therefore allowed Microsoft to determine, at least to an extent, the types of those data. Some of these same types of personal data, without specification of such types of data under the 2021 ILA,[362] are then further processed for various Microsoft's own business purposes. First by carrying out pseudonymisation and aggregation, followed by additional processing intended to achieve those business purposes. The 2021 ILA does not specify how those data will be processed to achieve any of the stated purposes. It follows that with regard to processing for Microsoft's own business purposes, Microsoft is, to a significant extent, determining the means of the processing. In particular, which types of personal data are processed for which purpose and how they are processed.

189. Moreover, when an entity engages in processing of personal data as part of its interactions with its own employees, customers, or members, it will generally be the one determining the purpose and means of the processing and therefore acting as a controller.[363]

190. Microsoft's preferred way of calculating employee compensation and compensation of its partner incentives forms part of Microsoft's own relationship with its employees. It is for Microsoft to determine how personal data are processed for this purpose by reference to its own needs;[364] not for the Commission to do so. Nor can the Commission be responsible for how Microsoft carries out its accounting, prepares business forecasts, reports internally, develops its product offering[365] or draws up its annual accounts. While the Commission may participate in the determination of the purposes and means of the processing as regards *basic* billing[366] and account management,[367] the EDPS nonetheless considers that the Commission does not solely determine such purposes and means but rather does so together with Microsoft Ireland. This is because it is for the provider of

---

[360] Reply by Microsoft Ireland of 26 May 2023, para. 192.

[361] See para. 177 of this decision.

[362] See, to that effect, judgment in Case C-25/17, *Jehovan todistajat*, EU:C:2018:551, para. 68, judgment in Case C-807/21, *Deutsche Wohnen*, ECLI:EU:C:2023:950, para. 41, and judgment in Case C-683/21, *Nacionalinis visuomenės sveikatos centras*, ECLI:EU:C:2023:949, para. 30.

[363] Cf. EDPB Guidelines 07/2020, para. 27.

[364] Cf. reply by Microsoft Ireland of 26 May 2023, Annex 4, p. 14.

[365] Cf. reply by Microsoft Ireland of 26 May 2023, Annex 4, p. 14.

[366] Such billing could entail calculating the amount of its usage of services billed per volume or per user and involve processing of personal data that are strictly necessary for that calculation. The full extent of billing, in addition to information provided by Microsoft Ireland in its reply of 26 May 2023, Annex 4, has not been revealed to the EDPS.

[367] Account management entails assessing aggregated information about the usage which it only sometimes shares with the Commission (reply by Microsoft Ireland of 26 May 2023, Annex 4, p. 13).

services to determine, at least partially, the modalities of processing of personal data related to billing and account management.

191. Microsoft's business operations processing is naturally attached to the pursuit of its own interests. It cannot therefore be said that Microsoft is acting "*on behalf of*" the Commission.[368] Microsoft's role is not limited to choosing the most appropriate technical and organisational measures applicable the processing (non-essential means of the processing).[369] It acts with a high degree of independence, for example in deciding what information to use and how to use it, thus determining at least some of the essential means in addition to the purposes of the business operations processing, as also noted in paragraph 188.[370]

192. Moreover, Microsoft Ireland states that:

> "*[the update to the DPA] clarifies that Microsoft accepts the additional, applicable responsibilities as a data controller when Microsoft processes data for the specified administrative and operational [business] purposes incident to providing the products and services (although Microsoft also accepts that a customer may consider that processing is subsumed under the customer's instructions to Microsoft as its processor).*"[371]

The EDPS understands this statement as an indication that, in principle, Microsoft considers itself to be controller as regards processing of personal data for its own business purposes.[372] It follows that with regard to at least some, if not the majority of its customers, Microsoft considers that it determines the purposes and means of the processing for its own business purposes. The EDPS is of the view that this further suggests that the contractual assignment of controllership for such processing does not correspond to the actual determination of its purposes and means. Even though Microsoft is willing to accept that the Commission as its customer considers itself the controller, Microsoft nonetheless considers itself controller for essentially the same types of processing operations vis-à-vis some of its other customers. In view of the above, the EDPS considers this to be a factor in substantiating that the contractual assignment of controllership was done purely formalistically and not in line with the actual circumstances.

193. As noted in paragraphs 120 and 161 of this decision, prior to the amendment of 19 December 2023, Microsoft Ireland was carrying out processing operations in a way

---

[368] Cf. the EDPB's description of acting "*on behalf of*" a controller, Guidelines 07/2020, paras. 79-81.

[369] Cf. the EDPB's position that acting "*on behalf of*" a controller may still leave a degree of discretion to choose the most suitable technical and organisational means, EDPB Guidelines 07/2020, para. 80.

[370] Any natural or legal person who exerts influence over the processing of personal data, for their own purposes, and who participates, as a result, in the determination of the purposes and means of that processing, is to be regarded as a controller in respect of such processing. In that regard [and without prejudice to the obligation to comply with Article 29 of the Regulation], it is not necessary that the purposes and means of processing be determined by the use of written guidelines or instructions from the controller, nor is it necessary for that controller to have been formally designated as such. See, to that effect, judgment in Case C-683/21, *Nacionalinis visuomenės sveikatos centras*, ECLI:EU:C:2023:949, para 30, judgment in Case C-807/21, *Deutsche Wohnen*, para. 41, and judgment in Case C-25/17, *Jehovan todistajat*, EU:C:2018:551, paras. 67 and 68.

[371] Reply by Microsoft Ireland of 26 May 2023, Annex 4, p. 7. Microsoft Ireland also states that: "due to customer and regulatory input, [Microsoft] recognize[s] some would construe this processing as operating as a controller." (Ibid., Annex 4, p. 16).

[372] Notwithstanding the statement by Microsoft Ireland referred to in para. 187 of this decision.

that was inconsistent with the applicable ILA. The EDPS considers that this further substantiates that Microsoft Ireland was itself determining those business operations purposes of the processing. Moreover, Microsoft Ireland has also been determining at least part of the essential means, since it is the one determining what types of personal data are to be processed for those purposes and with whom[373] those data are shared.

194. In view of the foregoing and without prejudice to the joint or separate nature of the controllership, the EDPS considers that Microsoft acts as a controller in respect of all four Microsoft's business purposes under the DPA.[374]

195. This conclusion is unaffected by a statement in the DPA that the processing for these purposes is "*incident to delivery of the Online Services*".[375]

196. The EDPS does not consider that any of these purposes could be incidental to delivery of the services,[376] with the exception of using basic billing and account data to obtain payment for them. Microsoft's preferred way of calculating employee compensation and partner incentives forms part of Microsoft's relationship with its employees and partners, respectively. It is not subordinate to providing EU institutions or bodies with ICT solutions; nor does it occur fortuitously in the context of Microsoft providing those solutions. The Commission's 2021 DPIA confirms that processing for Microsoft's internal reporting, forecasting and business modelling activities is partly grounded in its need to "*understand the needs of its customers and [...] develop new tools and pricing models,*"[377] which is unnecessary to provide the services that EU institutions or bodies already subscribe to. This is all the more the case given that "*ongoing improvement*" of all services provided by Microsoft forms part of the definition of service provision agreed by the Commission and Microsoft.

197. Accessorily, this is further corroborated by findings by other public authorities in the EU in relation to Microsoft 365.

198. According to the Dutch Ministry of Justice, Microsoft has stated:

> "*We already provide many intelligent services, combined with a service component. There is no question that we will analyse patterns and practices not only to improve security, but also to investigate whether there are new tools we want to build, also*

[373] E.g. partners for billing and account management and for calculating partner incentives; stakeholders for Microsoft internal reporting and business modelling; stakeholders and the market for financial reporting.

[374] The EDPS does not take a position on whether processing for which Microsoft acts as a controller complies with the GDPR, which is for the competent supervisory authorities in Member States to determine, taking into account also the EDPS' findings (see, to that effect, case-law of the Court of Justice in Case C-645/19 (*Facebook Ireland and Others*) and in Case C-252/21 (*Meta Platforms and Others (Conditions générales d'utilisation d'un réseau social)*).

[375] Commission's email of 19 December 2023, Annex 2 (Amendment to Contract Documents), pp. 1 and 2. With regard to business operations purposes related to provision of software and professional services, see also pp. 4 and 5 of the amendment. This amendment did not contain substantive modifications in this regard to the Section on "*Processing for Microsoft's Business Operations*" in the main body of the DPA, 2021 ILA, p. 29, or to respective sections related to the provision of software and professional services, pp. 53 and 66. See in this respect also reply by Microsoft Ireland of 26 May 2023, Annex 4, p. 2, first para., p. 7, third para., and p. 8, fourth para.

[376] See EDPB Guidelines 07/2020, section 2, pp. 9-18.

[377] Commission's 2021 DPIA, p. 77. See also reply by Microsoft Ireland of 26 May 2023, Annex 4, p. 23, point b).

based on competitors, and questions from customers. This has to be possible. We will use data to the max, within what the law allows us."[378]

This confirms that Microsoft considers it an essential commercial interest to process large amounts of data to develop new services. Processing for this purpose is not, however, incidental to delivery of the services.

199. German data protection authorities have reached similar conclusions in their assessment of Microsoft 365 on how Microsoft's own purposes of processing are set out in the September 2022 Data Processing Agreement.[379] Other data protection authorities, such as the Greek one, have identified similar issues.[380]

3.1.2.4. Processing for (in)compatible purposes and intra-EEA transmissions

200. Under Articles 4(1)(b) and 6 of the Regulation, the Commission has a duty to ensure that personal data processed on its behalf are not further processed in a manner that is incompatible with the purposes for which they were initially collected. Under Article 4(2) of the Regulation, it must be able to demonstrate that this is the case.

201. Any transmission of personal data by the Commission within the EEA must comply with Article 9 of the Regulation. This includes transmissions of personal data to Microsoft that were initiated by the Commission as well as those requested by Microsoft, regardless of whether Microsoft further processes such data as a controller or processor.[381]

202. In order for a transmission of personal data to comply with Article 9(1)(b) and (2) of the Regulation, it must be established that it is necessary to transmit those data for a specific purpose in the public interest. Where there is any reason to assume that the data subject's legitimate interests might be prejudiced, it must additionally be established that it is proportionate to transmit the personal data for that specific purpose after having demonstrably weighed the various competing interests. This means that the Commission must demonstrate that the transmission of those data is necessary for and proportionate to the tasks that it carries out in the public interest.

203. In its preliminary assessment, the EDPS considered that it was not feasible for the Commission to have made the assessment required under Articles 6 and 9 of the Regulation. The EDPS considered this because, as detailed in sections 3.1.2.1 and 3.1.2.2, the Commission had not determined the purposes of the processing in sufficiently specified and explicit terms, or clearly determined the types of personal data to be

---

[378] The Dutch Ministry of Justice's DPIA of Office 365 ProPlus, 22 July 2019, p. 64.

[379] See the findings of the Conference of German DPAs on Microsoft Online Services (Microsoft 365), 24 November 2022, in summary (pp. 3, 4 and 5) and assessment (pp. 10, 11, 13, 14 and 15). See similarly the findings of the Baden-Württemberg DPA's audit of Microsoft 365 in the context of a pilot project on its possible use in schools (23 April 2021, published 25 April 2022), in particular in the Baden-Württemberg DPA's opinion (p. 6, 7, 8, 10 and 11).

[380] See in this respect the EDPB report on the 2022 Coordinated enforcement action on the use of cloud-based services by the public sector, 17 January 2023, in particular findings by the Greek and Lithuanian DPAs in annex (pp. 50, 51, 53, 95 and 96).

[381] See also EDPB Guidelines 07/2020, footnote 76, p. 45. See in this respect also the EDPB report on the 2022 Coordinated enforcement action on the use of cloud-based services by the public sector, 17 January 2023, pp. 13, 15 and 30.

processed. The EDPS concluded that the Commission had therefore infringed those Articles of the Regulation.

204. With regard to compliance with **Article 6** of the Regulation, the Commission rejects that preliminary finding "*as it is based on factual incorrectness with regard to the determination of the types of personal data and purposes of processing*".[382] It further states that:

> "*As explained in sections 1.2.2. and 1.2.3 the Commission clearly established the types of personal data and purposes of processing for the provision of Customer with the Online Services in the ILA as well as in the Record of processing.*"[383]

In view of the findings set out in sections 3.1.2.1 and 3.1.2.2 of this decision, and in particular that the Commission has failed to specify the types of personal data and the purposes of the processing as required by the Regulation, the EDPS rejects this statement as inaccurate. Without such specification, it is not feasible for the Commission to have carried out an assessment whether the purposes of further processing are compatible with the purposes for which the personal data were initially collected.

205. With regard to compliance with **Article 9** of the Regulation, the Commission raises an objection to the applicability of that provision to transmissions of personal data to processors.[384] In this regard, it states that:

> *"The Commission, as controller, must in general ensure that the intended processing of personal data has a legal ground and is necessary and proportionate in the light of the objectives pursued. Once this is established, the transmission of personal data from the Commission to a processor does not require a second assessment of necessity and proportionality, which would be the consequence when applying Article 9 of the Regulation.*[385]
>
> *What counts is that the controller, when making use of a processor, meets the requirements of Article 29. Article 29 ensures that the controller only makes use of processors that provide sufficient guarantees in such a manner that processing will meet the requirements of the Regulation. It also requires the controller-processor relationship be governed by a contract. Article 29(3) contains the elements which should be included in the contract. With Article 29 the EU legislator has made sure that the protection offered by the Regulation is ensured when EU institutions make use of a processor.*[386]
>
> *There is no indication that the EU legislator, in addition, intended to apply Article 9 to this particular relationship. The transmission from the controller to the processor is inherent to the choice of making use of a processor. The only assessment to be made in such a case is whether the controller meets the requirements of Article 29 when doing so."*[387]

---

[382] Commission's reply of 25 May 2023, para. 80.
[383] Commission's reply of 25 May 2023, para. 80.
[384] Commission's reply of 25 May 2023, para. 82.
[385] Commission's reply of 25 May 2023, para. 83.
[386] Commission's reply of 25 May 2023, para. 84.
[387] Commission's reply of 25 May 2023, para. 85.

The EDPS rejects the Commission's objection and considers that Article 9 fully applies to transmissions of personal data to processors,[388] for the following reasons.

206. First, Article 9 of the Regulation provides for conditions which must be complied with for any transmissions to **recipients** established in the EU other than EU institutions and bodies. According to Article 3(13) of the Regulation, a 'recipient' is a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, **whether a third party or not**.[389] According to Article 3(14) of the Regulation, a third party is a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.[390] It follows that the notion of recipient under the Regulation clearly includes processors. The Commission has not provided any arguments disputing that interpretation. The additional qualifier set out in Article 9(1) of the Regulation only excludes recipients, including processors, that either are not established in the EU or are EU institutions and bodies. Microsoft Ireland and any of sub-processors in the EU do not fall in either of those excluded categories. Transmissions of personal data to them are therefore subject to Article 9 of the Regulation.

207. Second, the controller must indeed ensure that any processing of personal data has a valid ground for lawfulness under Article 5 of the Regulation and must ensure that the processing is necessary and proportionate in view of the objectives it pursues, as stated by the Commission. However, it cannot be inferred merely from this obligation that the controller is not required to satisfy the specific conditions for transmissions set out in Article 9 of the Regulation. Such an interpretation would run counter to the wording and intent of that provision. The legislature has clearly decided to require that additional conditions be met for certain intra-EEA transmissions (i.e. intra-EEA transmissions by and on behalf of EU institutions or bodies) compared to other processing. Given that there is no corresponding provision in the GDPR, additional safeguards are deemed necessary, under the Regulation, in view of the nature and responsibilities of EU institutions and bodies.[391] Indeed, the intention of Article 9 is to provide "*for a specific level of protection*"[392] to the transmission of personal data to recipients referred to in that provision.

208. Third, the fact that the controller must ensure compliance with other provisions of the Regulation, such as, with regard to processors, Article 29, does not affect its obligation to comply with Article 9 of the Regulation. The EDPS acknowledges that complete and effective compliance with Article 29 of the Regulation may well be a factor in the assessment required under Article 9 thereof. But compliance with Article 29 of the Regulation must not be interpreted as implying that Article 9 may simply be ignored as regards transmissions to processors that are not EU institutions or bodies. The EDPS is of the view that such an interpretation would be *contra legem* as there is no ground

---

[388] In so far as they are established in the EU and are not EU institutions and bodies, as provided for in Article 9 of the Regulation.

[389] The GDPR contains a similar definition of 'recipient' in Article 4(9).

[390] The GDPR contains a similar definition of 'third party' in Article 4(10).

[391] See also recital 28 of the Regulation and para. 215 of this decision.

[392] Proposal for a regulation of the European Parliament and of the Council on the protection of individuals 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 (COM/2017/08 final - 2017/02 (COD)), Explanatory Memorandum, Section 5.

either in Article 9 or Article 29 that compliance with the latter absolves the controller from complying with the former, as suggested by the Commission.

209. In its reply to the preliminary assessment, Microsoft Ireland states that Implementing Decision (EU) 2021/915 laying down Article 29 SCCs does not contain a reference to Article 9 of the Regulation, nor did the EDPS refer to it in its "*commentary*" to the Article 29 SCCs.[393] The EDPS understands the "*commentary*" as referring to the EDPB-EDPS Joint Opinion 1/2021.[394] On this basis, Microsoft Ireland suggests that Article 9 of the Regulation is not a "*requirement to consider in this context*".[395]

210. The EDPS rejects this argument for the following reasons.

211. First, Article 29(3) and (4) of the Regulation provide for requirements as to what must be stipulated in the contract between the controller and the processor. Implementing Decision (EU) 2021/915 sets out SCCs that fulfil those requirements.[396] Conversely, Article 9 of the Regulation does not regulate that contractual relationship. Instead, it imposes an obligation on the controller to ensure that the requirements as regards necessity and proportionality provided therein have been met. It is therefore logical that Implementing Decision (EU) 2021/915 does not contain a specific reference to Article 9 of the Regulation.

212. Second, Implementing Decision (EU) 2021/915 sets out SCCs that fulfil not only the requirements laid down in Article 29(3) and (4) of the Regulation but also in Article 28(3) and (4) GDPR. The Commission has explained in recital 2 of that Implementing Decision that the same set of standard contractual clauses should apply in respect of the relationship between controllers and processors subject to the GDPR and also when they are subject to the Regulation. In that same recital, the Commission has also explained that this is because data protection rules in both Regulations have, as far as possible, been aligned with each other.[397] It follows that any specificities of the Regulation, such as Article 9 which does not have a corresponding provision in the GDPR, were in any event not included in that Implementing Decision. This must, however, not be construed as meaning that the controller under the Regulation is not required to comply with Article 9 of the Regulation when transmitting data to processors in the EEA that are not EU institutions and bodies.

213. The Commission further states that even if Article 9 of the Regulation were applicable, the Commission would in any event not be in breach of that Article.[398] According to the Commission, it was able to carry out an assessment under Article 9 of the Regulation and "*has implemented the necessary contractual, organizational and technical as established in the DPIA*".[399]

---

393 Reply by Microsoft Ireland of 26 May 2023, para. 195.

394 EDPB - EDPS Joint Opinion 1/2021 on the European Commission's Implementing Decision on standard contractual clauses between controllers and processors for the matters referred to in Article 28(7) of Regulation (EU) 2016/679 and Article 29(7) of Regulation (EU) 2018/1725.

395 Reply by Microsoft Ireland of 26 May 2023, para. 195.

396 Article 1 of Implementing Decision (EU) 2021/915 provides that that Implementing Decision sets out SCCs that fulfil the requirements for contracts between controllers and processors laid down in Article 28(3) and (4) GDPR and Article 29(3) and (4) of the Regulation.

397 See also recital 5 of the Regulation.

398 Commission's reply of 25 May 2023, paras. 86, 87 and 94.

399 Commission's reply of 25 May 2023, paras. 86, 87 and 93.

214. The EDPS rejects the Commission's statement that it was able to carry out an assessment under Article 9 of the Regulation. Explicit and specified purposes of the processing and types of personal data set out as required by the Regulation are a pre-condition for any such assessment. This flows not only from the essential character of the purposes of the processing and the types of personal data in the context of any processing under the Regulation, but also from Article 9 itself. As provided for in Article 9(2) of the Regulation, where the controller initiates the transmission under that Article, it must demonstrate that the transmission of **personal data** is necessary for and proportionate to the **purposes** of the transmission.[400] Without first having sufficiently specified the personal data to be transmitted and the purposes of the transmission, any assessment under Article 9 of the Regulation would have been incomplete. Therefore, the necessity and proportionality required under that provision could not have been established. In view of the findings set out in sections 3.1.2.1 and 3.1.2.2 of this decision, and in particular that the Commission has failed to specify the types of personal data and the purposes of the processing as required by the Regulation, the EDPS maintains that the Commission has not complied with Article 9 of the Regulation.

215. Accordingly, the EDPS rejects as irrelevant statements made by the Commission and Microsoft Ireland aiming to establish why it is necessary and proportionate to transmit the personal data, in particular, to support the management and functioning of the Commission.[401] The EDPS acknowledges that the management and functioning of EU institutions and bodies, including the Commission, is considered as a task carried out in the public interest within the meaning of Article 5(1)(a) of the Regulation.[402] EU institutions and bodies may therefore rely on that Article as a ground for lawfulness with regard to processing of personal data necessary for their management and functioning, provided that Article 5(2) of the Regulation is complied with. However, the requirements under Article 9 of the Regulation should be understood as supplementary to the conditions for lawful processing under Article 5 thereof.[403] As noted above, an assessment under Article 9 requires that the personal data and the specific purposes of the transmission must first be specified as required by the Regulation.[404] It is not sufficient, in the context of that assessment, to rely on the purpose of management and functioning of the Commission,[405] stated necessity to use products which the Commission staff is "*familiar*" with,[406] "[*adherance*] *to the principle of efficiency and modernisation*"[407] or "*specific principles on sound financial management and performance*".[408] These are not the purposes of the processing, including transmission, of the personal data to Microsoft Ireland or sub-processors in the EEA under the 2021 ILA.

216. The EDPS therefore maintains that the Commission has infringed Articles 6 and 9 of the Regulation as set out in paragraph 203 of this decision.

---

[400] Similarly also provided for in Article 9(1)(b) that refers to the necessity of having the "**data** transmitted" for a "specific **purpose** in the public interest".

[401] Commission's reply of 25 May 2023, paras. 87 to 94, supplemented by its statements at the hearing of 23 October 2023, and reply by Microsoft Ireland of 26 May 2023, paras. 196 to 205, and Annex 4.

[402] See also recital 22 of the Regulation.

[403] Recital 28 of the Regulation.

[404] This is without prejudice to the assessment under Article 5 of the Regulation.

[405] Commission's reply of 25 May 2023, paras. 88 and 89, and reply by Microsoft Ireland of 26 May 2023, paras. 196 and 197.

[406] Commission's reply of 25 May 2023, paras. 90 and 92.

[407] Reply by Microsoft Ireland of 26 May 2023, para. 202. See also Commission's reply of 25 May 2023, para. 94.

[408] Reply by Microsoft Ireland of 26 May 2023, para. 198.

3.1.3. Findings

217. In view of the foregoing, the EDPS finds that the Commission, on the reference date and continuously thereafter until the date of issuing this decision:

a) has infringed Article 4(1)(b) of the Regulation by failing to:

- sufficiently determine the types of personal data collected under the 2021 ILA in relation to each of the purposes of the processing so as to allow those purposes to be specified and explicit;

- ensure that the purposes for which Microsoft is permitted to collect personal data under the 2021 ILA are specified and explicit;

b) has infringed Article 29(3)(a) of the Regulation by insufficiently determining in the 2021 ILA which types of personal data are to be processed for which purposes and by failing to provide sufficiently clear documented instructions for the processing;

c) has infringed Articles 4(2) and 26(1) in conjunction with Article 30 of the Regulation by failing to ensure that Microsoft processes personal data to provide its services only on documented instructions from the Commission;

d) has infringed Article 6 of the Regulation by failing to assess whether the purposes for further processing are compatible with the purposes for which the personal data have initially been collected;

e) has infringed Article 9 of the Regulation by failing to assess whether it is necessary and proportionate to transmit the personal data to Microsoft Ireland and its sub-processors (including affiliates) located in the EEA for a specific purpose in the public interest.

3.2. International transfers

3.2.1. Applicable law

218. Article 46 of the Regulation provides that:

> *"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 this Regulation, the conditions laid down in this Chapter 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 this Chapter shall be applied in order to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined."*

219. Article 47(1) of the Regulation provides that:

> *"1. A transfer of personal data to a third country or international organisation may take place where the Commission has decided pursuant to Article 45(3) of Regulation*

(EU) 2016/679 or to Article 36(3) of Directive (EU) 2016/680 that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection and where the personal data are transferred solely to allow tasks within the competence of the controller to be carried out."

220. Article 48(1), 2(b) and (c) and 3(a) of the Regulation provides that:

> *"1. In the absence of a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 or to Article 36(3) of Directive (EU) 2016/680, 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.*
>
> *2. The appropriate safeguards referred to in paragraph 1 may be provided for, without requiring any specific authorisation from the European Data Protection Supervisor, by:*
>
> *(b) standard data protection clauses adopted by the Commission in accordance with the examination procedure referred to in Article 96(2);*
>
> *(c) standard data protection clauses adopted by the European Data Protection Supervisor and approved by the Commission pursuant to the examination procedure referred to in Article 96(2);*
>
> *3. Subject to the authorisation from the European Data Protection Supervisor, the appropriate safeguards referred to in paragraph 1 may also be provided for, in particular, by:*
>
> *(a) 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;"*

221. Article 29(3)(a) of the Regulation provides that:

> "3. *Processing by a processor shall be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the subject matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller. That contract or other legal act shall stipulate, in particular, that the processor:*
> (a) *processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by Union or Member State law to which the processor is subject.*"

222. Article 31(1)(d) of the Regulation provides that:

> *"Each controller shall maintain a record of processing activities under its responsibility. That record shall contain all of the following information: [...] the categories of recipients to whom the personal data have been or will be disclosed*

including recipients in Member States, third countries or international organisations."

223. Recital 22 of the Regulation states that:

> *"[...] Processing of personal data for the performance of tasks carried out in the public interest by the Union institutions and bodies includes the processing of personal data necessary for the management and functioning of those institutions and bodies. [...]"*

224. Recital 63 of the Regulation states that:

> "*When personal data are transferred from the Union institutions and bodies to controllers, processors or other recipients in third countries or to international organisations, the level of protection of natural persons ensured in the Union by this Regulation should be guaranteed. The same guarantees should apply in cases of onward transfers of personal data from the third country or international organisation to controllers, processors in the same or another third country or international organisation. [...]*"

225. Recital 70 of the Regulation states that:

> "*In any case, where the Commission has taken no decision on the adequate level of data protection in a third country, the controller or processor should make use of solutions that provide data subjects with enforceable and effective rights as regards the processing of their data in the Union once those data have been transferred so that that they will continue to benefit from fundamental rights and safeguards.*"

226. Chapter V of the Regulation lays down rules governing transfers of personal data within the scope of the Regulation to third countries and international organisations.

227. Chapter V of the GDPR contains analogous rules for transfers that are within the scope of the GDPR.

3.2.2. Analysis

3.2.2.1. Requirements under the Regulation for international transfers

Transfers of personal data outside the EEA. Requirements of Article 46 of the Regulation.

228. Article 46 of the Regulation sets out the general principle for 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, including onward transfers. The Regulation does not provide a definition of a transfer. As the EDPB is tasked under Article 70(1)(e) GDPR to issue guidelines, recommendations and best practices in order to encourage consistent application of the GDPR, it has provided guidance to clarify the notion of a transfer. According to the EDPB,[409] a processing operation may be qualified as a transfer when three cumulative criteria are met:

[409] EDPB Guidelines 05/2021 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).

1) a controller or a processor ('exporter') is subject to the GDPR [the Regulation as regards transfers by and on behalf of EU institutions or bodies] 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 country, irrespective of whether or not this importer is subject to the GDPR [or the Regulation] for the given processing in accordance with Article 3, or is an international organisation.[410]

229. The EDPS concurs with the EDPB and considers that a processing operation which meets the above three cumulative criteria qualifies as a transfer. If such a transfer is envisaged under a contract, a transfer tool under Chapter V of the Regulation must be relied upon for any such transfer to occur. Transfers envisaged under a contract are transfers that the controller knows or should foresee in the broader context of the execution of the contract, or under other organised relationship.[411]

230. In that vein, remote access from a third country[412] constitutes a transfer, provided that the three above-mentioned criteria are met.[413] Equally, remote governmental access[414] under third-country laws to personal data located and processed in the EEA results in transfers of personal data.[415]

Need to carry out a transfer mapping to comply with Article 46, in particular in light of Article 48 of the Regulation

231. According to Article 46 of the Regulation, a controller may only allow transfers of personal data to take place if they comply with the Regulation.[416] The controller must therefore assess whether transfers would be compliant and what measures are necessary to ensure their compliance, including with Article 48 of the Regulation in the absence of an adequacy decision.[417] To be able to make such an assessment, the controller must first have a clear understanding of what personal data are (or are proposed to be) transferred, to which recipients, in what destinations and for what purposes.[418] This includes an assessment of the risks of remote access from third countries or international organisations to personal data stored in the EEA and any onward transfers of data transferred from the EEA.[419]

---

[410] EDPB Guidelines 05/2021, point 9. See also EDPS Decision of 13 July 2023 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, para. 31.
[411] See EDPS Decision of 13 July 2023, para 32.
[412] When it actually takes place.
[413] EDPB Guidelines 05/2021, point 16.
[414] When it actually takes place.
[415] By analogy see point 24 of the EDPB Guidelines 05/2021. See also EDPS Decision of 13 July 2023, para. 33.
[416] See also recital 63 of the Regulation.
[417] See paras. 131 to 133 of the *Schrems II* judgment.
[418] EDPB Recommendations 01/2020 of 18 June 2021 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, section 2.1, paras. 8 to 12.
[419] See EDPB Recommendations 01/2020, para. 13.

232. The transfer-mapping exercise and verifications must be carried out before any transfer is made, and updated prior to resuming transfers following their suspension.[420] They are also necessary to discharge the controller's duty of accountability.[421]

233. In its reply to the preliminary assessment, Microsoft Ireland states that:

> "*Transfer 'mapping' is not an explicit legal requirement under the EUDPR. The EUDPR only requires controllers and processors, at Art. 31, to keep an internal record of relevant processing including transfer activities*". [422]

> "*The requirement to perform transfer mapping in any event does not rest [with] the Commission because it is not the exporter.*"[423]

234. The EDPS rejects these arguments. The fact that the wording 'transfer mapping' does not appear in the Regulation does not mean that the Regulation does not require that such mapping be carried out. In this regard, the EDPS refers to paragraph 231 of this decision. The EDPS stresses that without having complete awareness of which types of data are transferred to which recipients in what destinations and for what purposes, it is not possible to make an assessment necessary to ensure compliance with the Regulation, and in particular to ensure an essentially equivalent level of protection.[424] This includes any safeguards and measures necessary to ensure such a level of protection.

235. Moreover, the EDPS notes that Article 31 of the Regulation does not serve a purpose identical to the purposes of Articles 46 and 48 thereof. Nor are the requirements following from those Articles as regards documenting information related to transfers of the same scope. Indeed, any information gathered when complying with Article 31 of the Regulation may be used to assist with compliance with Articles 46 and 48 thereof. Nevertheless, the information to be contained in the record of processing activities, in principle, does not suffice to ensure that an essentially equivalent level of protection is ensured for personal data transferred to third countries, as explained above. Furthermore, the EDPS did not allege an infringement of Article 31 of the Regulation in the preliminary assessment, nor does the EDPS find such an infringement in this decision.

236. According to the *Schrems II* judgment, it is for the controller or processor to provide appropriate safeguards in the absence of an adequacy decision.[425] This includes mapping of transfers as a pre-condition for ensuring such safeguards, as explained above. However, the interpretation provided by the Court of Justice, and in particular that also the processor is to provide appropriate safeguards, must be regarded in light of the key provisions of the Regulation. Under Article 4(2) of the Regulation, the controller is responsible for compliance with Article 4(1) and bears the burden of demonstrating its compliance with each of the principles set out Article 4(1) of the Regulation.[426] Under

---

[420] See also EDPB Recommendations 01/2020, para. 12. Transfer mapping is step 1 of the roadmap set out in EDPB Recommendations 01/2020.

[421] Articles 4(2) and 26(1) of the Regulation. See also EDPB Recommendations 01/2020, para. 8.

[422] Reply by Microsoft Ireland of 26 May 2023, para. 221. See also para. 213.

[423] Reply by Microsoft Ireland of 26 May 2023, para. 231. See also para. 222.

[424] See Articles 46 to 48 of the Regulation in light of the *Schrems II* judgment.

[425] *Schrems II* judgment, para. 131.

[426] See, to that effect, judgment in Case C-60/22, *Bundesrepublik Deutschland*, ECLI:EU:C:2023:373, paras. 32 and 53, and judgment in Case C-175/20, *Valsts ieņēmumu dienests (Processing of personal data for tax*

Article 26(1) of the Regulation, the controller must also implement appropriate technical and organisational measures to ensure and be able to demonstrate that the processing is performed in accordance with the Regulation and that the implemented measures are effective.[427] This includes transfers that are carried out by the controller or by others on its behalf. It therefore follows from Articles 4 and 26 of the Regulation that the responsibility for compliance with the Regulation, including Articles 46 to 48, lies with the controller. This responsibility encompasses ensuring that the pre-conditions for complying with those provisions, such as mapping of transfers, are satisfied. This conclusion is without prejudice to whether in this specific case there are direct transfers from the Commission to a third country, and in particular to Microsoft Corporation in the United States, which is analysed below.

237. In its reply to the preliminary assessment, Microsoft Ireland acknowledges that the transfer mapping requirement was "*further illustrated*" with the adoption of the Commission Implementing Decision (EU) 2021/914[428] setting out SCCs for transfers.[429] Microsoft Ireland specifically refers to Clause 14(b)(i) of those SCCs which provide that the parties must take due account of:

> "*the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred.*"[430]

Microsoft Ireland, however, adds that:

> "*The SCCs are a contractual measure that apply intra [sic] partes, as and when a party signs up to the SCCs, and do not impose any direct legal or regulatory requirements.*"[431]

The EDPS concurs that the SCCs have an inherently contractual nature. However, appropriate safeguards as required by the GDPR may be provided by those SCCs only if all clauses set out in the Implementing Decision are maintained. It follows from recital 109 GDPR that clauses may be added, provided that they do not contradict, directly or indirectly, the SCCs or prejudice the fundamental rights or freedoms of data subjects. Conversely, the controller or processor must not remove any clauses if it wishes to rely on the SCCs when ensuring appropriate safeguards. The Commission was vested by the EU legislator with the power to adopt, under Article 46(2)(c) GDPR, SCCs that

---

purposes), EU:C:2022:124, paras. 77, 78 and 81, as well as the judgment in Case C-77/21, *Digi*, ECLI:EU:C:2022:805, para 24, and the Opinion of the Advocate General Pikamäe in that case (ECLI:EU:C:2022:248), point 47. See also EDPB Binding Decision 3/2022 on the dispute submitted by the Irish SA on Meta Platforms Ireland Limited and its Facebook service (Art. 65 GDPR), para. 105, EDPB Binding Decision 4/2022 on the dispute submitted by the Irish SA on Meta Platforms Ireland Limited and its Instagram service (Art. 65 GDPR), para. 108, and EDPB Binding Decision 5/2022 on the dispute submitted by the Irish SA regarding WhatsApp Ireland Limited (Art. 65 GDPR), para. 101.

[427] See, in this respect also recital 45 of the Regulation.

[428] 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, 7.6.2016, p. 31). Despite being named standard *contractual* clauses by the Commission, these are standard *data protection* clauses adopted pursuant to Article 46(2)(c) GDPR.

[429] Reply by Microsoft Ireland of 26 May 2023, para. 220.

[430] Reply by Microsoft Ireland of 26 May 2023, para. 220.

[431] Reply by Microsoft Ireland of 26 May 2023, para. 220.

provide for appropriate safeguards required under the GDPR. It follows that as a controller, the Commission cannot choose to ignore a clause from the SCCs, as suggested by Microsoft Ireland, in so far as it wishes to rely on those SCCs when its processor transfers personal data on its behalf.

Requirement of Article 47(1). Specific purpose limitation for transfers under the Regulation

238. As transfers of personal data out of the EEA may generate additional risks for data subjects, they are subject to specific rules under Chapter V of the Regulation. The general principle enshrined in Article 46 of the Regulation underscores that transfers are subject to the Regulation as a whole: the level of protection afforded by the Regulation must travel with the data.[432] That level of protection must not be undermined.

239. This implies, in particular, that all transfers, including onward transfers, as any form of processing must comply with Articles 4, 5 and 6 of the Regulation, along with Article 10 if the processing involves special categories of data. The controller must therefore follow a two-step process: first, it must ensure that a valid legal basis underpins the transfer, and that it complies with all relevant provisions of the Regulation; second, it must comply with Chapter V.[433]

240. By adopting an adequacy decision under the GDPR or Directive (EU) 2016/680,[434] the Commission decides that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question, for the purpose of Article 45 GDPR or Article 36 of Directive (EU) 2016/680, ensures an adequate level of protection for personal data transferred from the EEA. Transfers to organisations in third countries or to international organisations covered by the adequacy decision can take place without the need to obtain any further authorisation. However, it is still necessary to comply with all the other provisions of EU data protection law.[435] When transfers take place by or on behalf of an EU institution or body, this means compliance must be ensured with all the provisions of the Regulation, including the second condition of Article 47(1).

241. Article 47(1) of the Regulation imposes two cumulative conditions on the transfer of personal data outside the EEA: first, a Commission adequacy decision must cover the jurisdiction in question, and second, the transfer must take place "*solely to allow tasks within the competence of the controller [i.e. EU institution or body][436] to be carried out.*" In

---

[432] See also recital 63 of the Regulation, paras. 134 and 214 of the Opinion 1/15 (*EU-Canada PNR Agreement,* ECLI:EU:C:2017:592), para. 73 of the *Schrems I* judgment (*Schrems*, C-362/14, ECLI:EU:C:2015:650) and paras. 92 to 94 of the *Schrems II* judgment.

[433] See e.g. EDPB Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679, p. 3, and EDPB Guidelines 2/2020 on articles 46 (2) (a) and 46 (3) (b) of Regulation 2016/679 for transfers of personal data between EEA and non-EEA public authorities and bodies, para. 6.

[434] 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).

[435] See, in this respect, recital 64 and Article 46 of the Regulation.

[436] Article 3(8) of the Regulation defines the "controller" as the EU institution or body or its organisational entities. The second condition of Article 47(1) of the Regulation therefore refers to competences of EU institutions or bodies and not to competences of "controllers other than [EU institutions or bodies]" defined

view of recital 22 of the Regulation, such tasks should be interpreted, in particular, as tasks carried out in the public interest, including the management and functioning of the EU institution or body concerned.

242. The second condition in Article 47(1) is particular to the Regulation and distinguishes transfers under it from transfers under the GDPR. It imposes an additional purpose limitation specific to transfers, reflective of the status EU institutions and bodies as public service institutions.[437]

243. That purpose limitation is a necessary condition: if a transfer is not necessary for the controller institution to carry out its tasks, the transfer must not take place. It recalls the strict purpose limitations imposed by Articles 4, 5 and 6 of the Regulation and the purpose limitation provided for transmissions to recipients within the EEA by Article 9 of the Regulation.

Requirements of Article 48 of the Regulation. Effective appropriate safeguards.

244. Under Article 48(1) of the Regulation, in the absence of an adequacy decision covering the jurisdiction of the destination, controllers and processors may transfer personal data to a third country[438] only if appropriate safeguards are provided, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available. Standard data protection clauses ('SCCs') adopted by the Commission, or by the EDPS and approved by the Commission, may provide for such appropriate safeguards.[439] Such safeguards may also be provided, subject to the authorisation from the EDPS, by contractual clauses between the controller or processor on the one hand and the controller, processor or the recipient of the personal data in the third country or international organisation on the other (so-called "*ad hoc* contractual clauses").[440]

245. These transfer tools 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 EEA by EU data protection law, read in the light of the Charter.[441]

246. There are currently no standard data protection clauses adopted pursuant to Article 48(2)(b) or (c) of the Regulation. The standard contractual clauses for the transfer of personal data to third countries pursuant to the GDPR (adopted on 4 June 2021) only allow processors processing on behalf of EUIs to avail themselves of that decision adopted under the GDPR. At least for direct transfers to third countries, EU institutions

---

in Article 3(9) of the Regulation (i.e. not to competences of controllers as defined in Article 4(7) of the GDPR).

[437] Article 94(1) of the Regulation imposes a similar condition for transfers of operational data: "*Subject to restrictions and conditions laid down in the legal acts establishing the Union body, office or agency, the controller may transfer operational personal data to an authority of a third country or to an international organisation* ***insofar as such transfer is necessary for the performance of controller's*** [i.e. EU institution's or body's] ***tasks*** *and only where the conditions laid down in this Article are met*" (emphasis added).

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

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

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

[441] See paras. 96 and 103 of the *Schrems II* judgment and recitals 65 and 70 and Article 46 of the Regulation. Identifying the transfer tool being relied on is step 2 of the roadmap set out in EDPB Recommendations 01/2020.

or bodies should therefore seek to rely on *ad hoc* contractual clauses in accordance with Article 48(3)(a) of the Regulation.

247. The EDPS takes the view that also where the transfer in question is not covered by an adequacy decision, but by appropriate safeguards, the purpose limitation referred to in Article 47(1) of the Regulation does not fall away. This reading is supported by the *Schrems II* judgment[442] which makes clear that a transfer subject to appropriate safeguards must benefit from the same level of protection as a transfer under an adequacy decision. For EU institutions and bodies, that level of protection includes the purpose limitation under Article 47(1) of the Regulation,[443] otherwise personal data transferred on the basis of appropriate safeguards could be subject to a lesser level of protection than personal data transferred under an adequacy decision. This would contradict the objective of Chapter V of the Regulation which is the same as the objective of Chapter V GDPR as interpreted by the Court of Justice: ensuring the continuity of the protection of personal data. Therefore, EU institutions and bodies must comply with such purpose limitation in addition to the requirements of Article 48 of the Regulation. In light of the level of protection guaranteed by Articles 4, 5, 6, 9 and 46 of the Regulation, even a transfer subject to appropriate safeguards should take place "*solely to allow tasks within the competence of the controller to be carried out.*"[444] It is therefore incumbent on the EU institution or body to limit the purposes for which it or its (sub-)processors transfer data out of the EEA to purposes without which the EU institution or body cannot carry out its tasks.

248. In its reply to the preliminary assessment, Microsoft Ireland objects to this view on the ground that this purpose limitation is provided in Article 47 and not in Article 46 or 48 of the Regulation.[445] The EDPS rejects this objection for reasons referred to in paragraph 247, which already take into account that the purpose limitation is stipulated in Article 47 of the Regulation. The specific purpose limitation under Article 47(1) must be interpreted in light of Articles 4, 5, 6, 9 and 46 of the Regulation.

249. Moreover, Microsoft Ireland puts forward that because Microsoft is not an EU institution or body, it is not subject to the Regulation but rather to the GDPR.[446] Microsoft Ireland therefore states that the purpose limitation provided in Article 47 of the Regulation in any event does not apply to transfers from Microsoft Ireland to Microsoft Corporation [in the Commission's use of Microsoft 365] because the GDPR applies to those transfers and the GDPR does not contain such a requirement.[447]

250. The EDPS rejects those arguments. It follows from Article 29 of the Regulation that processors must meet the requirements of the Regulation. Furthermore, the Commission cannot circumvent the provisions of the Regulation by not imposing upon processors acting on its behalf those provisions of the Regulation which are specific to it and additional to the provisions of the GDPR. In any event, the EDPS notes that the

---

[442] See paras. 92 to 94 and 96 of the *Schrems II* judgment.

[443] This reading is also supported by Article 94(1) of the Regulation which clearly imposes a similar purpose limitation condition for transfers of operational data under an adequacy decision (point a) of Article 94(1)) and for transfers of operational data under appropriate safeguards transfer tools (points b) and c) of Article 94(1)).

[444] Article 47(1) of the Regulation, read in the light of Articles 4, 5, 6, 9 and 46 thereof.

[445] Reply by Microsoft Ireland of 26 May 2023, para. 264.

[446] Reply by Microsoft Ireland of 26 May 2023, para. 247.

[447] Reply by Microsoft Ireland of 26 May 2023, para. 263.

2021 ILA provides that Microsoft is a processor under the Regulation,[448] not under the GDPR. The specific provisions of the Regulation which are not reflected in the GDPR, such as Article 47(1) of the Regulation, therefore fully apply to processing operations, including transfers, carried out by Microsoft Ireland on behalf of the Commission.

251. To provide appropriate safeguards within the meaning of Article 48(1) of the Regulation, an EU institution or body as a controller can use as a basis the SCCs for transfers under the GDPR,[449] in particular their module two for transfers controller to processor, to *prepare* contractual clauses under Article 48(3)(a) of the Regulation.[450] However, an EU institution or body cannot directly rely on the SCCs for transfers under the GDPR, even as *ad hoc* contractual clauses.

252. The EU institution or body needs to adapt the SCCs for transfers under the GDPR considering the role of the EU institution or body as a public authority carrying out its tasks in the public interest under EU law. The clauses must therefore reflect all the requirements of the Regulation. In particular, the clauses should reflect:

    a) stricter purpose limitation requiring that personal data are transferred solely to allow tasks within the competence of the EU institution or body to be carried out under EU law,[451]
    b) stricter limitation on onward transfers,[452]
    c) increased obligations to ensure security and confidentiality of personal data and electronic communications,[453]
    d) supervision by the EDPS of compliance of the processing of transferred personal data with the Regulation.

253. More generally, in order to be able to ensure the required continuity of the protection, the EU institution or body as a controller must remain in control of the whole processing.[454]

254. The contractual clauses subscribed by the EU institution or body must be binding on all entities involved (processor, its establishments, affiliates, partners and sub-processors). Those clauses must clearly detail (e.g. in annexes) for all envisaged recipients[455] which personal data from which services will be transferred,[456] for which purpose, to which recipients in which third country, with which safeguards and measures; as well as

---

[448] 2021 ILA, pp. 26 and 30. In another part of its reply to the preliminary assessment, Microsoft Ireland acknowledges that Microsoft acts as a processor under the Regulation (Annex 5, para. 82). Under 2021 ILA, Microsoft also undertakes to comply with several provisions of the Regulation (e.g. on pp. 32, 35). Moreover, the 2021 ILA provides that Microsoft acknowledges the investigative powers of the EDPS under Article 58 of the Regulation (p. 36).

[449] Set out in Implementing Decision (EU) 2021/914.

[450] If EU institutions or bodies use the SCCs for transfers under the GDPR, they are deemed to be *ad hoc* contractual clauses for transfers within the meaning of Article 48(3)(a) of the Regulation. This corresponds to how the use by EU institutions or bodies of the SCCs for transfers under Directive 95/46/EC was deemed as *ad hoc* transfer clauses under Article 9(7) of Regulation 45/2001 (see EDPS guidance on transfers of personal data to third countries by EU institutions, p. 22).

[451] Stemming from Article 47(1) of the Regulation.

[452] Stemming from Articles 46, 47(1) and 6 of the Regulation. Moreover, the Regulation does not provide for legitimate interests ground for processing or legitimate interests derogation for transfers.

[453] Stemming from Articles 33 and 36 of the Regulation.

[454] See Articles 26, 29 and 46 and recitals 45 and 63 of the Regulation.

[455] Processor's establishments, its affiliates, partners and sub-processors.

[456] Whether by way of a transfer to a third country, remote access to personal data within the EU from a third country or onward transfers within the same or to another third country.

instructions of the EU institution or body in that regard.[457] The clauses must also impose clear and binding obligations on all envisaged recipients[458] in third countries to which personal data will be transferred by the EU institution or body.

255. The EU institution or body must therefore take into account the results of the transfer-mapping exercise and transfer impact assessment[459] it has carried out. To reflect the requirements enunciated in the *Schrems II* judgment, whenever necessary, the clauses must include contractual supplementary measures and commitments on technical and organisational supplementary measures, identified by the EU institution or body in its transfer impact assessment.

256. In addition, the clauses should provide for the possibility for other recipients (e.g. other establishments or entities of the corporate group and other sub-processors) to whom personal data will be transferred to accede to the clauses. If other recipients do not accede to the clauses, the EU institution or body must take further action to obtain sufficient guarantees from the processor and sub-processor, as explained in paragraphs 258 and 259.

257. EU institutions or bodies as controllers must obtain authorisation by the EDPS pursuant to Article 48(3)(a) of the Regulation before they can rely on *ad hoc* contractual clauses to transfer directly personal data outside of the EEA.

258. If the EU institution or body has allowed its processor to transfer personal data to other processors and sub-processors in third countries for processing on the institution's behalf, these sub-processors can accede to the *ad hoc* contractual clauses between the EU institution or body and the processor under Article 48(3)(a) of the Regulation. If they do not, the processors of EU institutions or bodies may use the processor to processor module of the SCCs for transfers under the GDPR in so far as those SCCs are adapted to reflect the clauses concluded between the EU institution or body and its processor.[460] The SCCs for transfers under the GDPR also set out rights and obligations with respect to matters referred to in Article 28(3) and (4) GPDR (equivalent to Article 29(3) and (4) of the Regulation).[461] Such SCCs therefore have to be adapted to reflect also the data protection obligations as set out in the contract between the EU institution or body and its processor under Article 29(3) of the Regulation.[462]

259. In both cases,[463] the EU institution or body as the controller for the whole processing must obtain sufficient guarantees that the processor has implemented appropriate contractual, technical and organisational measures with other processors'

---

[457] See also the explanatory note that opens the appendix to the SCCs for transfers under the GDPR in Implementing Decision (EU) 2021/914.

[458] Processor's establishments, its affiliates, partners and sub-processors.

[459] As explained in paras. 260 to 271 of this decision.

[460] This means including additional provisions in the contractual clauses concluded between the processor and third-country sub-processors and thereby adapting the SCCs for transfers under the GDPR to reflect the clauses concluded between the EU institution or body as the controller and that processor. See also recital 66 of the Regulation and recitals 3 and 8 of Implementing Decision (EU) 2021/914.

[461] Article 1(2) of Implementing Decision (EU) 2021/914.

[462] Article 29(4) of the Regulation requires that: "*where a processor engages another processor for carrying out specific processing activities on behalf of the controller, the same data protection obligations as set out in the contract or other legal act between the controller and the processor as referred to in paragraph 3 shall be imposed on that other processor by way of a contract or other legal act under Union or Member State law*". In this respect, see also recital 8 of Implementing Decision (EU) 2021/914.

[463] Accession to *ad hoc* clauses under Article 48(3)(a) of the Regulation or use of adapted SCCs adopted under Article 46(2)(c) GDPR.

establishments, affiliates, partners and sub-processors. The EU institution or body has to satisfy itself that such measures implemented for transfers to other recipients:

a) correspond to the role and the processing of transferred personal data the recipient will carry out on behalf of the EU institution or body,
b) are in line with the assessments made and supplementary measures identified by the EU institution or body during its transfer impact assessment, and
c) will be implemented by the processor and sub-processors.

Need for the controller to conduct a transfer impact assessment to provide the appropriate safeguards necessary to ensure compliance with Articles 46 and 48 of the Regulation

260. In line with Article 46 of the Regulation, as clarified in the *Schrems II* judgment, data subjects whose personal data are transferred outside of the EEA under appropriate safeguards must be afforded a level of protection essentially equivalent to that which is guaranteed within the EEA.[464]

261. Pursuant to the *Schrems II* judgment, where the transfer relies on a transfer tool under Article 48 of the Regulation or Article 46 GDPR (i.e. under 'appropriate safeguards'), the EU institution or body acting as a controller must carry out an assessment to determine whether, in the context of the specific transfer and taking into account the transfer tool relied on, the third country of destination affords the transferred data an essentially equivalent level of protection to that in the EEA.[465] In particular, the controller must assess whether any legislation or practices of the third country, applicable to the transferred data and/or the data importer, interfere with the data importer's ability to comply with its commitments made in the transfer tool, taking into account the circumstances surrounding the transfer.[466]

262. The EDPB has clarified what the requirements stemming from EU data protection law are in light of the *Schrems II* judgment to ensure a level of protection essentially equivalent to that in the EEA, in EDPB Recommendations 01/2020,[467] and specifically as regards access by third-country authorities for surveillance purposes in EDPB Recommendations 02/2020.[468] The final version of EDPB Recommendations 01/2020 was adopted and published on 18 June 2021. However, a first version of those Recommendations was adopted and published for public consultation on 10 November 2020.[469]

263. The assessment referred to in paragraph 261 may reveal that the legislation or practices of the third countries concerned are problematic in terms of their effect on the appropriate safeguards envisaged by the transfer tool to ensure an essentially equivalent level of protection.

---

464 *Schrems II* judgment, paras. 94 and 96.
465 *Schrems II* judgment, paras. 104, 105, 133 and 134.
466 Step 3 of the roadmap in EDPB Recommendations 01/2020.
467 Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data.
468 Recommendations 02/2020 on the European Essential Guarantees for surveillance measures.
469 Those EDPB Recommendations became applicable immediately following their publication. The EDPS considers this to be relevant to the reply by Microsoft Ireland of 26 May 2023, para. 269.

264. In line with the *Schrems II* judgment and EDPB Recommendations 01/2020, the EDPS understands 'problematic legislation' to be legislation that:

a) imposes on the recipient of personal data from the EU obligations and/or affect the data transferred in a manner that may impinge on the transfer tools' contractual guarantee of an essentially equivalent level of protection; and

b) does not respect the essence of the fundamental rights and freedoms recognised by the Charter or exceeds what is necessary and proportionate in a democratic society to safeguard one of the important objectives as also recognised in EU or Member State law, such as those listed in Article 25(1) of the Regulation.

By analogy, 'problematic practices' should be understood in the same way.

265. As stated by the EDPB in its Recommendations 01/2020,

"*public authorities in third countries may endeavour to access transferred data:*

a) In transit by accessing the lines of communication used to convey the data to the recipient country. This access may be passive in which case the contents of the communication, possibly after a selection process, are simply copied. The access may, however, also be active in the sense that the public authorities interpose themselves into the communication process by not only reading the content, but also manipulating or suppressing parts of it.

b) While in custody by an intended recipient of the data by either accessing the processing facilities themselves, or by requiring a recipient of the data to locate, and extract data of interest and turn it over to the authorities."[470]

Such access may affect the security and confidentiality of personal data which must be ensured under Articles 33 and 36 of the Regulation.

266. In its assessment, an EU institution or body must take into consideration the specific circumstances of the transfer (e.g. types 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 transfer-mapping exercise. It should also take account of any onward transfers that are envisaged.[471]

267. If the legislation or practice of the third country is problematic as referred to in paragraph 264, the EU institution or body must establish whether contractual, technical and organisational measures exist to supplement the transfer tool effectively ('supplementary measures').[472] It can do this in collaboration with its processor and the data importer.

---

[470] EDPB Recommendations 01/2020, para. 80.

[471] See Article 46 of the Regulation, paras. 104 and 134 of the *Schrems II* judgment, and paras. 33 and 34 of EDPB Recommendations 01/2020.

[472] See EDPB Recommendations 01/2020, para. 54 and Annex 2. Identifying and implementing effective supplementary measures is step 4 of the roadmap in EDPB Recommendations 01/2020. See also para. 133 of the *Schrems II* judgment.

268. Supplementary measures will be required where problematic legislation or practices[473] in the third country, such as relating to access by public authorities of that third country to transferred data, prevent an essentially equivalent level of protection, as guaranteed by appropriate safeguards under the transfer tool, from being afforded to the transferred personal data.[474]

269. This process of assessing the level of protection in the third country, whether supplementary measures are needed and whether any effective supplementary measures exist is commonly called a **transfer impact assessment**. A methodology to conduct such an exercise is available in EDPB Recommendations 01/2020[475] and, as regards the assessment of access by public authorities for surveillance purposes, in EDPB Recommendations 02/2020.[476]

270. The EU institution or body as the controller must carry out the transfer impact assessment before any transfer is made or a suspended transfer is resumed, as without it, it is not possible to know the effective level of protection which will be afforded to the personal data transferred. The EU institution or body as the controller must carry out the transfer impact assessment for all transfers that are occurring or are envisaged under the contract with a processor, including implementing supplementary measures, where necessary.

271. In regard of the need for the EU institution or body as the controller to carry out a transfer impact assessment, Microsoft Ireland states that: "*the requirement to perform a [transfer impact assessment] rests [with] Microsoft Ireland*" because Microsoft Ireland is the exporter of the data.[477] The EDPS rejects this argument for the reasons already enunciated in paragraphs 231 to 237 of this decision. In particular, it follows from Articles 4 and 26 of the Regulation that the responsibility for compliance with the Regulation, including as regards carrying out a transfer impact assessment to ensure compliance with Articles 46 to 48, lies with the controller.

Need for effective supplementary measures to ensure compliance with Articles 46 and 48 of the Regulation

272. Where necessary, the EU institution or body must implement the supplementary measures it has identified in its transfer impact assessment to *effectively* ensure an essentially equivalent level of protection for the personal data transferred in that third country. This includes also ensuring that its processor and any recipient of transferred personal data implement supplementary measures that the EU institution or body has identified as required.

273. If the EU institution or body has identified that supplementary measures are needed to ensure an essentially equivalent level of protection for the personal data transferred in that third country, it must not proceed with the transfer without first implementing an

---

[473] See para. 264 of this decision.

[474] Articles 46 and 48 of the Regulation as interpreted in light of the Charter. See *Schrems II* judgment, paras. 131-134. See also EDPB Recommendations 01/2020, paras. 22 and 23.

[475] EDPB Recommendations 01/2020 of 18 June 2021 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data.

[476] EDPB Recommendations 02/2020 of 10 November 2020 on the European Essential Guarantees for surveillance measures.

[477] Reply by Microsoft Ireland of 26 May 2023, paras. 222, 270 and 271.

effective set of supplementary measures.[478] It must also ensure that its processor and recipient of transferred personal data have first implemented effective supplementary measures which the EU institution or body identified as necessary in its transfer impact assessment.

274. If the EU institution or body cannot implement supplementary measures that are required to ensure an essentially equivalent level of protection, it must not start transferring the data.[479] If it is already transferring data, the EU institution or body must end or suspend the transfer.[480]

275. As stated by the Court of Justice in the *Schrems II* judgment: "*That is the case, in particular, where the law of that third country imposes on the recipient of personal data from the European Union obligations which are contrary to those clauses and are, therefore, capable of impinging on the contractual guarantee of an adequate level of protection against access by the public authorities of that third country to that data.*"[481]

276. In its Recommendations 01/2020, the EDPB has identified five use case scenarios, describing specific circumstances and measures taken which the EDPB considers as effective supplementary measures to ensure an essentially equivalent level of protection:

- Use case 1 - data storage for backup and other purposes that do not require access to data in the clear;
- Use case 2 - transfer of pseudonymised data;
- Use case 3 - encryption of data to protect them from access by the public authorities of the third country of the importer when the data transit between the exporter and their importer;
- Use case 4 - protected recipient; and
- Use case 5 - split or multi-party processing.[482]

277. The measures identified by the EDPB in those use cases aim to preclude potentially infringing access by preventing the authorities from identifying the data subjects, inferring information about them, singling them out in another context, or associating the transferred data with other datasets that may contain, among other data, online identifiers provided by the devices, applications, tools and protocols used by data subjects in other contexts. For the use case scenarios where the EDPB has identified effective supplementary measures, the EDPB considers the measures applied are effective where public authorities in third countries may endeavour to access transferred personal data while in transit to or while in custody by the intended recipient of the data.[483]

278. If, however, all of the cumulative conditions set out in the respective five use case scenarios are not met, the measures cannot be considered effective. If the situation of the processing is different from the one covered by one of those five use case scenarios, the measures envisaged in the respective five use case scenarios might not be effective.

---

[478] EDPB Recommendations 01/2020, paras. 56 and 57.
[479] EDPB Recommendations 01/2020, para. 57.
[480] EDPB Recommendations 01/2020, para. 57.
[481] *Schrems II* judgment, para. 135.
[482] Annex 2 to EDPB Recommendations 01/2020, use cases 1 to 5 with effective supplementary measures.
[483] See, to that effect, EDPB Recommendations 01/2020, paras. 79, 80 and 81.

279. In its Recommendations 01/2020, the EDPB has identified two use case scenarios where the EDPB could not identify any effective supplementary measure to ensure an essentially equivalent level of protection:

- Use case 6 - transfer to cloud services providers or other processors which require access to data in the clear
- Use case 7 - transfer of personal data for business purposes including by way of remote access (and these data are not or cannot be effectively pseudonymised or effectively encrypted because the processing requires accessing data in the clear).[484]

3.2.2.2. Factual timeline related to the assessment of compliance of international transfers

280. On 30 October 2019, the Commission launched the first stage of a large-scale pilot of Microsoft 365, involving 500 staff members.[485]

281. On 10 March 2020, the EDPS issued its 2020 Findings and Recommendations.[486] Many of the serious concerns raised by the EDPS in the 2020 Findings and Recommendations concerning the compliance of using Microsoft software anticipated the *Schrems II* judgment.[487]

282. In May 2020, the Commission concluded a renegotiated ILA with Microsoft.[488]

283. On 1 June 2020, the Commission launched the second stage of the large-scale pilot of Microsoft 365, involving all members of its staff and the staff of several executive agencies.[489]

284. On 16 July 2020, the Court of Justice handed down the *Schrems II* judgment.

285. On 17 July 2020, Microsoft submitted to the EDPS for authorisation under Article 48(3)(a) of the Regulation a set of *ad hoc* contractual clauses for transfers "*from Microsoft*

---

[484] Annex 2 to EDPB Recommendations 01/2020, use cases 6 and 7 with no effective supplementary measure.
[485] Commission's additional reply of 7 June 2022, p. 10.
[486] See EDPS Public Paper on Outcome of own-initiative investigation into EU institutions' use of Microsoft products and services.
[487] Following its 2019-2020 investigation into the EU institutions' use of Microsoft products and services, the EDPS found a number of concerning areas of non-compliance, such as non-compliant data processing agreement, lack of control over use of sub-processors, lack of control over location of data processing and what was transferred out of the EEA and how, as well as a lack of proper safeguards to protect data that left the EEA and risk of unlawful disclosure of data. In its 2020 investigation report, the EDPS made a number of recommendations to the EU institutions (and bodies), including that the EU institutions (and bodies) should renegotiate their licence agreement and put in place contractual terms to clarify amongst others how to protect data being transferred. The EDPS made clear that – unless its recommendations were implemented - the contract with Microsoft should require that any processing of any personal data entrusted to Microsoft or its sub-processors by EU institutions (or bodies) should as a rule take place within the EU or the EEA. Moreover, the EDPS recommended that EU institutions (and bodies) should consider carefully any purchases of Microsoft products and services or new uses of existing products and services until after they have analysed and implemented the EDPS' recommendations. Where EU institutions (or bodies) planned to use Microsoft products and services they did not already use (such as Microsoft Office 365 or Microsoft Azure cloud services), they should perform comprehensive assessments of the data protection risks posed by those products and services prior to deploying them. See EDPS Public Paper on Outcome of own-initiative investigation into EU institutions' use of Microsoft products and services.
[488] Commission's substantive reply of 15 October 2021. p. 3; conclusion of amendment 4 to the ILA.
[489] Commission's additional reply of 7 June 2022, p. 10.

(as data exporter) and Microsoft Corporation (as data importer)" for the EU institutions' and bodies' use of Microsoft Online Services.

286. On 23 July 2020, the EDPS held a meeting with Microsoft to discuss its request for authorisation of the *ad hoc* contractual clauses. On 13 August 2020, the EDPS held a meeting with the Commission. During those meetings, the EDPS explained what information was needed to proceed with the request. Neither Microsoft nor the Commission pursued the matter.

287. On 11 September 2020, the Commission completed a transfer-mapping exercise.[490]

288. On 2 October 2020, the EDPS ordered all EU institutions and bodies to conduct a mapping exercise covering all of their international transfers and to report high-risk transfers to the EDPS.[491]

289. On 31 October 2020, the Commission completed a further transfer-mapping exercise in response to the EDPS' order.[492]

290. On 10 November 2020, the EDPB adopted a first version of its Recommendations 01/2020 for public consultation.[493]

291. On 2 December 2020, the Commission reported to the EDPS that high-risk transfers were taking place to the United States involving large-scale and complex processing in relation to its use of Microsoft products and services.[494]

292. On 7 May 2021, the Commission signed a revised ILA with Microsoft Ireland ('2021 ILA').[495]

293. In June 2021, the Commission and Microsoft Ireland concluded an amendment to the revised ILA, "*committing to insert new [standard contractual clauses ('SCCs')] once adopted*".[496]

294. On 18 June 2021, the EDPB adopted the final version of its Recommendations 01/2020.

295. In August 2021, the Commission implemented Double Key Encryption to protect documents that users labelled as sensitive non-classified.[497]

296. On 13 September 2021, Microsoft Ireland and Microsoft Corporation concluded SCCs on the basis of the SCCs set out in Implementing Decision (EU) 2021/914 (processor to processor module).[498]

---

[490] Commission's additional reply of 7 June 2022, p. 10.
[491] See EDPS' strategy for EU institutions to comply with the Schrems II judgment.
[492] Commission's additional reply of 7 June 2022, p. 10.
[493] EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data adopted on 10 November 2020 and open for public consultation until 21 December 2020. Those EDPB Recommendations became applicable immediately following their publication.
[494] Commission's letter of 2 December 2020.
[495] Commission's additional reply of 7 June 2022, p. 10.
[496] Commission's additional reply of 7 June 2022, p. 11.
[497] Commission's additional reply of 7 June 2022, p. 11.
[498] See the Commission's additional reply of 7 June 2022, Annex 1, pp. 58-78.

297. On 15 October 2021, the Commission completed its DPIA into the use of Microsoft 365 services in the Commission. The DPIA included a chapter entitled 'Transfer Impact Assessments'.[499]

298. On 8 November 2021, the Commission deployed Microsoft 365 services in full production throughout the institution and several executive agencies. The EDPS asked the Commission to clarify the significant differences between the large-scale pilot launched in June 2020 and the entry into full production.[500] The Commission has explained that the deployment in full production was distinguished by the implementation of Double Key Encryption and the accompanying authorisation given to staff to work on sensitive non-classified documents using Microsoft 365 software.[501]

299. In January 2022, the Commission and Microsoft Ireland concluded an amendment to the 2021 ILA.[502] According to the Commission, its stated objective was to "*reflect that SCCs [between Microsoft Ireland and Microsoft Corporation concluded on 13 September 2021] were fully implemented*".[503]

300. On 19 December 2023, the Commission and Microsoft Ireland concluded another amendment to the 2021 ILA.[504] That amendment, inter alia, made modifications to the DPA sections "Data Transfers", "Location of Customer Data at Rest" and "Disclosure of Processed Data".[505] The Commission has stated that: "*The changes do not introduce new or fundamentally different processing operations and therefore, by [its] understanding, no new facts to the investigation*".[506]

3.2.2.3. Compliance of transfers under 2021 ILA

The existence of direct transfers outside the EEA in the Commission's use of Microsoft 365

301. On the reference date, transfers of personal data in the Commission's use of Microsoft 365 were contractually permitted to occur in different ways: from Microsoft Ireland to Microsoft Corporation and other sub-processors,[507] and from the Commission to Microsoft Corporation and other sub-processors.[508] The latter followed, contractually,

---

[499] The Commission's additional reply of 7 June 2022, p. 10, states that the transfer impact assessment was completed on 30 June 2021, following EDPB Recommendations 01/2020 issued on 18 June 2021. However, the only documentary evidence of a transfer impact assessment the Commission has shared with the EDPS is dated 15 October 2021.

[500] EDPS letter to the Commission of 4 April 2022, p. 6.

[501] Commission's additional reply of 7 June 2022, p. 11.

[502] Commission's additional reply of 7 June 2022, Annex 1, pp. 58-78.

[503] Commission's additional reply of 7 June 2022, p. 11. This concerns the SCCs referred to in para. 296 of this decision. In its reply to the preliminary assessment, Microsoft Ireland also states that the January 2022 amendment to the DPA incorporated the SCCs concerned (Annex 5, para. 38; see also paras 39 and 40).

[504] Commission's email of 19 December 2023, Annex 2 (Amendment to Contract Documents).

[505] Commission's email of 19 December 2023, Annex 2 (Amendment to Contract Documents), pp. 2 to 5.

[506] Commission's email of 19 December 2023.

[507] 2021 ILA, pp. 45 and 46, where certain conditions are provided for transfers by "Microsoft". In 2021 ILA, p. 23, "Microsoft" is designated as "Microsoft Ireland Operations Limited". The transfers of personal data from Microsoft Ireland to Microsoft Corporation and other sub-processors follow the transmissions of such data from the Commission to Microsoft Ireland.

[508] 2021 ILA, Attachment 2 of the DPA, controller-processor SCCs, p. 72.

from the controller-processor SCCs on which the Commission relied on the reference date and which provided that the Commission (Customer) was the data exporter.[509]

302. In its 2021 DPIA and its reply of 15 October 2021, the Commission has stated that it "*does not transfer personal data to third countries directly.*"[510] In so far as this statement purports to pertain to the reference date, the EDPS rejects it for the following reasons.

303. **First**, both documents containing the statement that the Commission does not transfer personal data directly to third countries date from 15 October 2021. This is after the conclusion of 13 September 2021 of the processor to processor SCCs between Microsoft Ireland and Microsoft Corporation on the basis of the SCCs set out in Implementing Decision (EU) 2021/914.[511] Even though the 2021 ILA was formally modified by an amendment only in January 2022 to reflect the conclusion of those SCCs,[512] the 2021 ILA provided, prior to the conclusion of the amendment of January 2022, that:

> *"In case [...] the European Commission [...] adopt[s] standard data protection clauses for the transfers of personal data outside the European Union, in accordance with Article 48 par. 2(b) or (c) EUDPR and replacing Decision 2010/87/EU or the standard data protection clauses therein, such new standard data protection clauses shall be incorporated (**without separate amendment**) in the Attachment 2 of the DPA as of the day of their adoption, subject to final agreement on any adjustment the parties require to adapt the clauses adopted by the Commission to align with EUDPR, and shall replace the Standard Contractual Clauses as defined by the ILA."* (emphasis added)[513]

In view of this contractual provision, it may be considered that the processor to processor SCCs of 13 September 2021 had effectively already replaced the controller to processor SCCs when they were concluded. It follows that such a replacement occurred before the statement made on 15 October 2021 and quoted in paragraph 302. The EDPS therefore considers that that statement referred to the situation following the conclusion of the processor to processor SCCs. Consequently, that statement did no longer take into account the controller to processor SCCs which provided that the Commission was the data exporter. It follows that such statements are not relevant with regard to the reference date. This is supported by the fact that the statement in question does not specify reasons contesting the provision under the controller to processor SCCs according to which the Commission was the data exporter.

304. **Second**, the EDPS in any event considers that the controller to processor SCCs which were in force on the reference date, and until at least 13 September 2021, made it unequivocally clear that the Commission was the data exporter, with Microsoft Corporation as the importer.[514] In this regard, the EDPS considers that the absence, at the time of conclusion of 2021 ILA, of a Commission decision setting out processor to processor SCCs could not justify the usage of controller to processor SCCs[515] where, as

---

[509] 2021 ILA, Attachment 2 of the DPA, controller-processor SCCs, p. 72.
[510] 2021 DPIA, p. 94, and Commission's substantive reply of 15 October 2021, para. 2.7.8.
[511] See para. 296 of this decision.
[512] See para. 299 of this decision.
[513] 2021 ILA, p. 38.
[514] This is without prejudice to the findings below related to compliance with Article 48(3)(a) of the Regulation as regards those SCCs.
[515] As suggested by the Commission in the 2021 DPIA, p. 94, penultimate para, which states that: "*In the absence of Standard Contractual Clauses (processor to processor) at the time of signature of the ILA, the*

claimed by the Commission, no transfers were to take place between the controller and (sub-)processor.[516] Moreover, it was (and remains) possible for Microsoft to request authorisation of *ad hoc* processor to processor contractual clauses under Article 48(3)(a) of the Regulation for transfers taking place in the use of Microsoft products and services by EU institutions or bodies.[517] It follows that as of the reference date until at least 13 September 2021, the Commission was contractually permitted to transfer personal data to the Microsoft Corporation in the United States directly.

305. As noted above, on 13 September 2021, Microsoft Ireland and Microsoft Corporation concluded processor to processor SCCs, which replaced, in the 2021 ILA, controller to processor SCCs. This was reflected in the 2021 ILA by its amendment of January 2022.

306. According to the Commission and Microsoft Ireland, there have been no direct transfers from the Commission to third countries taking place also following the conclusion of the processor to processor SCCs.[518] The EDPS does not concur with that statement.

307. The EDPS has found that personal data are being transferred directly from the Commission's devices to servers in third countries, and in particular the United States. This finding is based on the information provided by Microsoft on its website, in particular on data location, on diagnostic and telemetry data collection, on different required or essential services, as well as on host domain names and IP address ranges for connection endpoints.[519] These findings are also corroborated by information provided in the reply by Microsoft Ireland of 26 May 2023 to the preliminary assessment, which further confirms that personal data are collected from users' devices[520] and sent

Standard Contractual Clauses 2010/87/EU (Controller to Processor) were used as appropriate safeguards […]."

[516] This is without prejudice to the findings below related to compliance with Article 48(3)(a) of the Regulation as regards those SCCs.

[517] In July 2021 and therefore after the initiation of the transfers under the 2021 ILA and after the reference date, Microsoft submitted for authorisation under Article 48(3)(a) of the Regulation a set of *ad hoc* contractual clauses, however it did not provide the EDPS with information required to proceed with handling of the authorisation request. See paras. 285, 286 and 493 of this decision.

[518] Commission' reply of 25 May 2023, para. 130, and the reply by Microsoft Ireland of 26 May 2023, para. 237.

[519] See, e.g. non-exhaustive information on pages on Microsoft's website concerning privacy controls for Microsoft 365 Apps for enterprise, concerning Microsoft 365 endpoints and Office 365 IP address ranges, as well as concerning collection of data about use of Microsoft 365 through Windows telemetry. Websites visited on 5 January, 30 March, 22 August and 20 December 2022 and on 31 January 2024. Several pieces of this information are also referred to in other parts of this decision.

[520] See, in this respect, reply by Microsoft Ireland of 26 May 2023, Annex 14 (Overview of privacy controls for Microsoft 365 Apps for enterprise, dated 27 March 2023), which also states that: "*Diagnostic data is collected and sent to Microsoft about Office client software running* ***on the user's device*** *in your organisation."* (p. 1) *"Even if you choose 'Neither', required service data will be sent* ***from the user's device*** *to Microsoft."* (p. 2) (emphasis added) *"[Microsoft's] system creates a unique ID that it associates with your user's diagnostic data."* (p. 2) *"As you use a connected experience, data is sent to and processed by Microsoft to provide you that connected experience. This data is crucial because this information enables us to deliver these cloud-based connected experiences."* (p. 5) *"There is also a set of services that are essential to how Microsoft 365 Apps for enterprise functions and cannot be disabled. [E.g.], the licensing service […] Required service data about these services is collected and sent to Microsoft, regardless of any other policy setting that you have configured".* (p. 6).

to Microsoft,[521] under transfer scenarios identified by the Commission in its 2021 DPIA.[522]

308. Moreover, in order to obtain further confirmation, in January 2023 (and again in February 2024), the EDPS carried out look-ups in relation to a number of connections identified by the Baden-Württemberg data protection authority in its audit of Microsoft 365 software[523] which is similar to that used by the Commission. Those connections identified by the Baden-Württemberg data protection authority and used to transmit personal data were made from the data protection authority's devices running Microsoft 365 software to Microsoft servers. The EDPS carried out the said IP look-ups of those servers and found that they were based in the United States.[524] The Commission and Microsoft Ireland did not specifically dispute the findings of these look-ups. In particular, they did not state that the connections identified by the Baden-Württemberg data protection authority's audit of Microsoft 365 software,[525] which is similar to that used by the Commission, were not occurring in the Commission's use of Microsoft 365. In fact, they both acknowledge that transfers take place from Microsoft software used by the Commission to the United States.[526] This demonstrates that in the Commission's use of Microsoft 365, personal data transmitted by the Microsoft 365 software installed on users' devices are in fact transferred outside of the EEA.

309. This understanding is also supported by reports issued by several other data protection authorities in the EEA[527] and by the Dutch Ministry of Justice.[528] Their reports include

---

[521] See, in this respect, also reply by Microsoft Ireland of 26 May 2023, Annex 5, paras. 94 and 98, and Annex 12 (Microsoft 365 Major Services Data Flows), p. 5. In particular, Microsoft Ireland has stated that: "*Diagnostic Data is* ***transferred outside the EU****, because Microsoft's core engineering and troubleshooting teams are located outside the EU, but always in pseudonymized and encrypted form.*" (Annex 5, para. 98, emphasis added).

[522] See, in this respect, paras. 344 to 357 of this decision.

[523] See the findings of the Baden-Württemberg DPA's audit of Microsoft 365 in the context of a pilot project on its possible use in schools (23 April 2021, published 25 April 2022), The Baden-Württemberg DPA found large data flows in its audit of Microsoft 365 (see annex 1, pp. 1 and 2). According to the findings of the audit, more than 517 different hosts were contacted in in total 112 006 requests (see annex 7, pp. 3, 11-96).

[524] Example of hosts identified by the Baden-Württemberg DPA are hosts such as "euc-word-edit.officeapps.live.com" (which made 11 098 requests), "outlook-1.cdn.office.net" (6167 requests), "teams.microsoft.com", "support.microsoft.com", "flow.microsoft.com" and "portal.azure.com". Looking up the six highlighted examples with tools https://mxtoolbox.com/ and https://www.iplocation.net/ip-lookup, it would appear these hosts and endpoints are based on servers located in the United States (EDPS checks on 10 and 12 January 2023, as well as on 5 February 2024).

[525] See the findings of the Baden-Württemberg DPA's audit of Microsoft 365 in the context of a pilot project on its possible use in schools (23 April 2021, published 25 April 2022), The Baden-Württemberg DPA found large data flows in its audit of Microsoft 365 (see annex 1, pp. 1 and 2). According to the findings of the audit, more than 517 different hosts were contacted in in total 112 006 requests (see annex 7, pp. 3, 11-96).

[526] See, in this respect, Commission's reply of 25 May 2023, para. 125, and reply by Microsoft Ireland of 26 May 2023, para. 256.

[527] See, in this respect, the findings of the Conference of German DPAs on Microsoft Online Services (Microsoft 365), 24 November 2022, in summary (pp. 7 and 8) and assessment (pp. 52 to 57). See similarly the findings of the Baden-Württemberg DPA's audit of Microsoft 365 in the context of a pilot project on its possible use in schools (23 April 2021, published 25 April 2022), in particular the analysis of the Baden-Württemberg DPA in its opinion (pp. 7, 10, 12 and 19), annex 1 (pp. 1 to 3 and 5 to 7), annex 7 (pp. 3, 11-96) and annex 10. See also the EDPB report on the 2022 Coordinated enforcement action on the use of cloud-based services by the public sector, 17 January 2023, in particular findings by the Cypriot, Greek and Lithuanian DPAs in annex (pp. 16 to 18, 52 to 55, 97).

[528] See, in this respect, the Dutch Ministry of Justice's DPIA of Office 365 ProPlus, 22 July 2019, pp. 8, 24, 32, 58, 66, 68 and 69. See also the Dutch Ministry of Justice's DPIA of Microsoft Teams, OneDrive, Sharepoint and Azure AD, 16 February 2022, pp. 9, 10, 19, 27, 34, 35, 37, 76-78, 93 and 111, the Dutch Ministry of Justice's DTIAs of on Microsoft Teams, OneDrive, Sharepoint and Azure AD, 21 February 2022, Tabs 1-7, pp. 1.

findings of their contractual analyses and technical tests of what data are collected and sent directly from users' devices during the use of Microsoft 365 software or its earlier versions.[529]

310. With regard to direct transfers, Microsoft Ireland states in its reply to the preliminary assessment that:

> *"[F]rom a technical, legal and organizational perspective, the M365 data always flows through Microsoft Ireland Operations Ltd. As the owner of the M365 software and the contracting party in the 2021 ILA, Microsoft Ireland Operations Ltd. is the Commission's processor (not Microsoft Corporation, which is a sub-processor), and the Commission, through using the M365 software which is owned and operated in the EU by Microsoft Ireland Operations Ltd., transfers the data to Microsoft Ireland Operations Ltd. and not to Microsoft Corporation."*[530]

The EDPS does not concur with this assessment. Where the controller uses services of the processor and the personal data related to such use flow directly from the device of the controller to a device or server in a third country, without going through a device or server of a processor located in the EEA, such a controller must be deemed as data exporter. The fact that such flows of personal data take place when the controller is using software that is owned and operated by the processor,[531] cannot be considered a decisive circumstance in determining the data exporter. An interpretation of the Regulation as to which entity is to be considered data exporter, as put forward by Microsoft Ireland, could lead to circumventing certain responsibilities of the controller when transferring personal data to a third country, simply by using a processor's software. This would be exacerbated by the fact that Microsoft Ireland considers that the controller, when the processor is the data exporter, is not responsible to perform transfer mapping[532] or a transfer impact assessment.[533]

311. Moreover, the EDPS does not consider that a direct contractual relationship is necessary between entities, such as the Commission and Microsoft Corporation, in order for there to be transfers between them from a legal perspective, as suggested by Microsoft Ireland.[534] Microsoft Corporation is the Commission's sub-processor[535] since Microsoft Ireland as the Commission's processor has a contractual relationship with Microsoft

---

[529] The Dutch Ministry of Justice and the Baden-Württemberg DPA carried out technical tests to detect and record outgoing telemetry and network traffic from users' devices in use of parts of the Microsoft 365 software or its earlier versions. The reports of the Dutch Ministry of Justice and of the Baden-Württemberg DPA give examples of hosts and endpoints to which the Ministry or the DPA found that data are sent in different events from users' devices.
The Dutch Ministry of Justice explains in e.g. its DPIA on Office 365 ProPlus (22 July 2019, p. 25 and 29) that it captured in total 226 different telemetry events and that the event "Office.Licensing.OfficeClientLicensing.DoLicenseValidation" was observed 228 times at the "Neither" (least telemetry) level. According to that DPIA (p. 70), Microsoft stated that "*Office telemetry contains between 23 and 25 thousand events*".
The Baden-Württemberg DPA found in its audit of Microsoft 365 that more than 517 different hosts were contacted in in total 112 006 requests (see annex 7, pp. 3, 11-96).

[530] Reply by Microsoft Ireland of 26 May 2023, para. 256. See also Commission's reply of 25 May 2023, para. 125.

[531] The EDPS notes that the Commission has a right to use Microsoft's software products and online services (2021 ILA, p. 15).

[532] Reply by Microsoft Ireland of 26 May 2023, para. 231.

[533] Reply by Microsoft Ireland of 26 May 2023, paras. 270, 271 and 276.

[534] Reply by Microsoft Ireland of 26 May 2023, paras. 241, 242 and 244.

[535] As also acknowledged by Microsoft Ireland in its reply of 26 May 2023, para. 246.

Corporation within the meaning of Article 29(4) of the Regulation. Without such a contractual relationship, Microsoft Corporation would not be permitted to carry out processing operations on behalf of the Commission in the Commission's use of Microsoft 365. The EDPS rejects as manifestly unfounded any claim that a controller, cannot proceed to a transfer of personal data to its sub-processor.

312. In this regard, Microsoft Ireland further states that:

> "*Microsoft has invested in endpoints for Diagnostic Data within the EU. As described in EU Data Boundary documentation (Annex 7), this applies to versions of Microsoft 365 Applications released after 31 December 2022. Thus, for customers who have updated to that version and later, there is no direct routing of M365 Diagnostic Data.*[536] *A limited exception to this is for Diagnostic Data from the Teams client, which, for a user associated with an EU customer may 'dual route' that data to both the EU and US.*[537]"

The EDPS does not consider this statement to be alleging or demonstrating that no direct transfers take place from the Commission to the United States. First, the statement only pertains to diagnostic data and not to other personal data being transferred, such as service generated data. Second, Microsoft Ireland acknowledges that even with regard to diagnostic data there is an exception as regards direct routing of data. Third, Microsoft Ireland refers to the EU Data Boundary which itself has a limited scope as further set out below and therefore only covers select types of personal data and processing operations. Fourth, the EDPS carried out its own examination described in paragraph 308 of this decision in January 2023, i.e. after the date referred to by Microsoft Ireland. In this regard, the EDPS has not received information demonstrating when the Commission's version of Microsoft 365 applications has been updated to the version referred to by Microsoft Ireland.

313. Microsoft Ireland further states that:

> "*[It] operates any account created under the M365 service offering, it operates the access rights in relation to the accounts, and any requests for remote access to EU official data are sent by or on behalf of Microsoft Ireland.*" [538]

In this regard, Microsoft Ireland refers to the EDPB Guidelines 05/2021[539] when stating that:

> "*[The EDPB] clarified that, in order to be considered a 'transfer', three cumulative legal conditions must be fulfilled. In doing so, the EDPB highlighted that the concept of a 'transfer' is a functional, legal and autonomous concept, which must be interpreted in light of EU data protection law – and this legal concept does not necessarily align with the strictly technical understanding of a transfer.*
>
> *The EDPB clarified that one of the conditions to a transfer is to 'disclose data by transmission' or otherwise 'making personal data available'. It clarified that the*

[536] Reply by Microsoft Ireland of 26 May 2023, para. 246.
[537] Reply by Microsoft Ireland of 26 May 2023, footnote 149 at the end of para. 246.
[538] Reply by Microsoft Ireland of 26 May 2023, para. 240.
[539] EDPB Guidelines 05/2021 on the interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR.

exporter could 'make data available' by taking the following (non-exhaustive) actions:

> *'creating an account, granting access rights to an existing account, "confirming"/"accepting" an effective request for remote access, embedding a hard drive or submitting a password to a file'*[540]".[541]

The EDPS considers that the application of the examples of making data available provided by the EDPB depends on all relevant circumstances of the situation at hand. In particular, in many instances the transfers are initiated by the Commission or its users, despite the Commission's statement to the contrary.[542] In fact the Commission acknowledges that at least certain diagnostic data are transferred "*only when [the related] functionalities are actively invoked by the users*".[543] This is the case when they reach out to support/helpdesk services in a third country by email, telephone or otherwise, or allow remote access to the personal data stored e.g. on the device or account of the Commission's user. This is the case also where the personal data, such as diagnostic data, are transferred, without the active involvement of Microsoft Ireland, from the devices of the Commission's users to devices or servers in a third country. It is only for the Commission as the controller to determine (and approve) which diagnostic data may be transferred to a third country. At least in those instances it cannot be considered that Microsoft Ireland discloses personal data to a recipient in a third country.

Insufficient documented instructions as regards to what personal data may be transferred and where. Violation of Article 29(3)(a) of the Regulation

314. In accordance with Article 29(3)(a) of the Regulation, processing, including transfers, by a processor must be governed by a contract or another legal act under EU or Member State law that is binding on the processor with regard to the controller. It follows from that Article that such a contract or legal act must, inter alia, set out the purpose of the transfer, types of personal data transferred, third countries concerned and recipients. In addition, the processor may processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by EU or Member State law to which the processor is subject. The EDPS examines compliance with that provision with regard to transfers carried out under the 2021 ILA, as follows.

Transfers on the reference date

315. The storage location of a portion of the data processed by Microsoft is specified in the DPA. The section of the DPA entitled "*Location of Customer Data at Rest*" provides that Microsoft will store data from the "*Core Online Services [...] within certain major geographic areas*" as listed in Chapter 1 of Attachment 1 to the DPA.[544]

---

[540] EDPB Guidelines 05/2021, para. 16.
[541] Reply by Microsoft Ireland of 26 May 2023, paras. 238 and 239.
[542] Commission's reply of 25 May 2023, para. 125. The Commission states that transfers are not actively initiated by the Commission.
[543] Commission's reply of 25 May 2023, para. 125.
[544] 2021 ILA, p. 37.

316. That Chapter contains a provision entitled "*Location of Customer Data at Rest for Core Online Services*" ('**EU Storage Guarantee**').[545] This allows the customer to control the storage location of a subset of "*Core Online Services*" data by either configuring its tenant in its desired geographic location or configuring the services to be deployed in that location.

317. As regards Office 365 data, Microsoft commits, under the 2021 ILA, to storing three groups of "*Customer Data*" in the EU: the Exchange Online mailbox content; the SharePoint Online site content; and files uploaded to OneDrive for Business.[546] Other file content and communication data from Office 365 services are not covered.

318. Also covered by the EU Storage Guarantee are Microsoft Azure Core Services, such as Azure Active Directory (which is used for the management of user identities in Microsoft Online Services). For these services, the 2021 ILA provides that in principle, data processed by Azure core services that qualify as "*Customer Data*" will be stored in the EU if the customer so chooses.[547] The 2021 ILA also makes clear, however, that: "*Certain services may not enable Customer to configure deployment in [the EU/EEA] or outside the United States and may store backups in other locations.*"[548] Microsoft may therefore transfer user directory information out of the EEA in ways that are not specified in the 2021 ILA. In its reply to the preliminary assessment, the Commission considers that these "*potential exceptions from the EU Storage Guarantee [...] are irrelevant*" because the services that it uses do not form part of those exceptions.[549] In this regard, the EDPS underlines the important distinction between permitted (and thus envisaged) transfers pursuant to a contract under Article 29(3) of the Regulation, which are examined here, and the factual circumstances which might ensure that the transfers, albeit permitted, do not actually take place. In particular, the objective of this section of the decision is not to demonstrate the existence of unspecified transfer scenarios, as suggested by the Commission,[550] but rather that transfers as referred to above are permitted under the 2021 ILA. Actual transfer scenarios are examined further below.

319. In this regard, the EDPS rejects the Commission's statement that "*Customer data will be stored at rest in the [EU]*"[551] as inaccurate. The Commission fails to take into account the provisions of 2021 ILA as referred to in paragraphs 317 and 318 of this decision that do allow transfers of Customer Data.

320. Moreover, the Commission states that:

> "*By default, no transfer of Customer Data may occur when **at rest**. When in use or in transit, transfers could occur only when this is necessary to deliver the service.*" (emphasis added)[552]

The EDPS considers that except for the case of remote access, personal data in general cannot be transferred while they are at rest (i.e. merely stored, without any additional

---

[545] 2021 ILA, pp. 45-46.
[546] Section on "*Location of Customer Data at Rest for Core Online Services*", 2021 ILA, pp. 45-46. The EDPS notes that according to the Product Terms site (as visited on 15 February 2024), the EU storage guarantee as regards Office 365 services includes Microsoft Teams chat messages and meeting recordings.
[547] 2021 ILA, pp. 45-46.
[548] 2021 ILA, pp. 45-46.
[549] Commission's reply of 25 May 2023, para, 118.
[550] Commission's reply of 25 May 2023, para, 118.
[551] Commission's reply of 25 May 2023, para, 114.
[552] Commission's reply of 25 May 2023, para, 114.

processing) since a transfer inherently entails that the data are not at rest. The Commission's statement that no transfers of [customer] data may occur when at rest therefore applies to any personal data, not just to personal data processed under the 2021 ILA, including customer data. It follows that the Commission's statement is superfluous. Moreover, the location of customer data at rest as provided under the 2021 ILA, in so far as such location is permitted to be outside the EEA, necessarily involves a prior transfer of such data. It is for this reason that the EDPS considers that personal data for which location at rest is permitted outside the EEA, are envisaged to be transferred under the 2021 ILA. As regards the second sentence of the quoted statement, the EDPS considers, in view of its generalised nature, that it does not contradict the EDPS' conclusions in this section. Transfers "*necessary to deliver the service*" are permitted (and thus envisaged) to occur under specific provisions of the 2021 ILA as referred to in this section.

321. Diagnostic data and service generated data (e.g. logs of application usage generated online, thus at server side) and other usage-related data are not covered by the EU Storage Guarantee.[553] Data processed to deliver professional services are not covered either.[554]

322. The EU Storage Guarantee therefore only covers a subset of the data processed as a result of the Commission's use of Microsoft 365. Precisely which types of personal data are covered by the guarantee cannot be clearly determined from the contract.

323. Indeed, the SCCs for transfers between the Commission and Microsoft Corporation incorporated into the 2021 ILA specified that the data to be transferred "*includes e-mail, documents and other data in an electronic form in the context of the Online Services.*"[555] The same types of data that benefit from the EU Storage Guarantee for Office 365, or at least a part of those data, may therefore also be transferred outside the EEA. There are no clear instructions in the 2021 ILA regarding the purposes for which such transfers may take place.[556]

324. Microsoft also commits to providing information on the physical location of data centres that are located within the EU in the 2021 ILA.[557] The 2021 ILA does not, however, provide for a mechanism for the Commission to obtain more information on what data are stored in the EEA than is already contained in the EU Storage Guarantee.

325. Microsoft makes no contractual commitments concerning the location of data that do not fall within the EU Storage Guarantee. Under the transfer provisions of the DPA and MBSA, Microsoft may transfer all personal data covered by the 2021 ILA to the United States or to any other country in which it or its sub-processors operate.[558]

---

[553] See definitions of "*Customer Data*", "*Diagnostic Data*", and "*Service Generated Data*", 2021 ILA, pp. 25-26. See also Commission's substantive reply of 15 October 2021, para. 2.6.5, p. 15, and Commission's 2021 DPIA, p. 28.

[554] See definition of "*Professional Services Data*", 2021 ILA, p. 26.

[555] 2021 ILA, p. 77.

[556] See in this respect similarly the findings of the Conference of German DPAs on Microsoft Online Services (Microsoft 365), 24 November 2022, in summary (pp. 3, 4) and assessment (pp. 7 to 11, 13 to 14, 54, 56).

[557] Section on "*Location of Customer Data at Rest*", 2021 ILA, p. 37.

[558] See clause 4(c) of the MBSA (2021 ILA p. 5), the section on "*Data Transfers*" in the body of the DPA (2021 ILA p. 38), the section on "*Data Transfers*" in the Software DPA Terms in Chapter 2 of Attachment 1 to the DPA (2021 ILA pp. 58-59), Chapter 3 of Attachment 1 to the DPA concerning standalone online services

326. The Commission has submitted that there are limits to what contractual commitments it can ask of Microsoft in the ILA.[559] It has pointed to the fact that the 2021 ILA has a duration of at least three years, and that the Commission must have the flexibility to make changes to its use of Microsoft services to reflect technical developments and its business needs.[560]

327. Whether they are included in the ILA or take another form, the Commission must require clear, exhaustive and binding information and commitments on where data at rest are located when it uses Microsoft 365. Without such information and commitments, the Commission cannot discharge its duty of accountability under the Regulation, rely knowingly on an appropriate transfer tool or negotiate safeguards and supplementary measures which might be necessary in each instance. Specifically, it cannot meet its obligations concerning transfers of personal data under Chapter V of the Regulation, as it is not in a position to perform the necessary assessment of the level of protection afforded to those data transferred outside the EEA. Likewise, it cannot fulfil its obligations concerning the use of processors and sub-processors, and the security and confidentiality of the processing, electronic communications and networks.[561] The provision of complex software services may require that the level of protection is assessed by grouping certain categories of data to be transferred according to objective criteria. However, without knowing at least where each category of data is stored, the Commission cannot know whether those data are transferred. It follows that the Commission cannot know whether it needs to take measures necessary to guarantee an essentially equivalent level of protection for those data, or necessary to ensure at least that the transfer can take place on the basis of derogations within the meaning of Article 50 of the Regulation, if the conditions for valid recourse to derogations are met.

Transfers after the reference date

328. After the reference date, the ILA was amended in January 2022 to reflect the processor to processor SCCs for transfers from Microsoft Ireland to Microsoft Corporation concluded on 13 September 2021 (see paragraphs 296, 299 and 303 of this decision).[562] According to the ILA as updated in January 2022, those processor to processor SCCs are a Microsoft intercompany agreement and may be updated from time to time, with any updates published on Microsoft's website.[563] The EDPS considers this possibility of changing the SCCs by Microsoft entities to be an indication that the ILA as updated in 2022 did not define clearly and comprehensively the exact scope of the transfers in the Commission's use of Microsoft 365, their purpose and each envisaged recipient (including subcontractors),[564] and the Commission's instructions in that regard. In this

(2021 ILA pp. 62-64) and the section on "Data Transfers" in Chapter 4 of Attachment 1 to the DPA, concerning professional services (2021 ILA p. 67).

559 Minutes of the evidence-gathering meeting held on 28 November 2021, p. 4.

560 Minutes of the evidence-gathering meeting held on 28 November 2021, p. 4.

561 See Articles 29, 33, 36 and Chapter V of the Regulation.

562 Commission's additional reply of 7 June 2022, Annex 1, pp. 58-78.

563 Commission's additional reply of 7 June 2022, Annex 1, p. 18. According to the DPA: "*For purpose of further clarity, 2021 Standard Contractual Clauses being a Microsoft intercompany agreement, may be updated from time to time. Updates to the 2021 Standard Contractual Clauses will provide at least equivalent levels of data protection as the current terms, attached for information purposes to this Data Protection Addendum in Attachment 7. The 2021 Standard Contractual Clauses, including any updates to these, are published and available for consultation on the Service Trust Portal (located at https://servicetrust.microsoft.com/ or its successor)*". It is not possible to access the 2021 SCCs between Microsoft Ireland and Microsoft Corporation, nor the International Data Transfer Addendum to these SCCs, without signing in to Microsoft's website.

564 See also the explanatory note that opens the appendix to the SCCs for transfers under the GDPR in

regard, the EDPS takes note of the Commission's statement that Microsoft cannot change those SCCs in a manner that would affect the scope of transfers, the type of data transferred or the recipients to which data are transferred[565] (i.e. essentials means of the processing). The EDPS notes, however, that despite Microsoft's general obligation under the 2021 ILA to only process personal data on documented instructions from the Commission, any future updates to the SCCs as envisaged by the 2021 ILA are not specifically limited to non-essential means of the processing. Moreover, Microsoft Ireland states that those SCCs were only appended to the 2021 ILA "*out of courtesy*",[566] which suggests that Microsoft Ireland does not consider the Commission's role in determining any changes to the SCCs as decisive.

329. The ILA was further amended on 19 December 2023, in particular modifying the sections "Location of Customer Data at Rest Data" and "Data Transfers".[567] Following that amendment, the DPA stipulates that the sub-processor agreements for transfers between Microsoft Corporation and its sub-processors provide the same level of data protection as implemented by Microsoft in the processor to processor clauses at Module III of the 2021 SCCs.[568] That amendment also provides that:

> *"For EU Data Boundary Online Services (as defined in the Product Terms), Microsoft will store and process Customer Data within the European Union and EFTA, unless as provided for by documented exceptions set out in the Product Terms."*[569]

330. Under the Product Terms site, EU Data Boundary means "*Microsoft computers, computing environment, and physical data centers located solely in the European Union (EU) and the European Free Trade Association (EFTA)*".[570] An extensive and exhaustive list of EU Data Boundary Services appears on the same website.[571] As stated by Microsoft Ireland:

> "*The EU Data Boundary [...] is a geographically defined boundary within which Microsoft has committed to store and process customer data for [Microsoft's] major commercial enterprise online services, including Azure, Dynamics 365, Power Platform, and Microsoft 365, subject to limited circumstances where customer data will continue to be transferred outside the EU Data Boundary.*"[572]

331. As further stated on the Product Terms site, the use of EU Data Boundary Services may result in various transfers of personal data, including customer data, outside the EU

Implementing Decision (EU) 2021/914.

565 Commission's reply of 25 May 2023, para. 134.

566 Reply by Microsoft Ireland of 26 May 2023, para. 249.

567 Commission's email of 19 December 2023, Annex 2 (Amendment to Contract Documents), pp. 3 and 4, points 5 and 6.

568 Commission's email of 19 December 2023, Annex 2 (Amendment to Contract Documents), pp. 3 and 4, point 6.

569 Commission's email of 19 December 2023, Annex 2 (Amendment to Contract Documents), p. 3, point 5.

570 Under the 2021 ILA, p. 3, the Product Terms site can be found at: https://www.microsoft.com/licensing/terms/product/PrivacyandSecurityTerms/EAEAS.

571 https://www.microsoft.com/licensing/terms/product/PrivacyandSecurityTerms/EAEAS.

572 Reply by Microsoft Ireland of 26 May 2023, para 71, and Annex 7A, p. 1. See also https://learn.microsoft.com/en-us/privacy/eudb/eu-data-boundary-learn.

Data Boundary.[573] In particular, diagnostic data, certain system-generated data,[574] and professional services data are not covered by the EU Data Boundary.[575] It cannot be determined from the contract or the Product Terms site precisely which types of personal data are covered by the EU Data Boundary. This is also because it is not specified under the 2021 ILA, as demonstrated in section 3.1.2.1, which types of personal data are contained in each of those categories of data. The EU Data Boundary is further analysed in paragraphs 496 to 508.

332. In this regard, the processor to processor SCCs of 13 September 2021 between Microsoft Corporation and Microsoft Ireland state that the following data are included in the categories of data that may be transferred under the SCCs: "*The personal data that is included in e-mail, documents and other data in an electronic form in the context of the Products and Services.*"[576] The same types of personal data that benefit from the EU Data Boundary, or at least a part of those data, may therefore also be transferred outside the EEA. There are no clear instructions in the 2021 ILA, also following the amendment of December 2023, regarding the purposes for which such transfers may take place.[577]

333. Moreover, Microsoft makes no contractual commitments, nor commitments on its Product Terms site, concerning the location of data that do not fall within the EU Data Boundary. Under the transfer provisions of the DPA and MBSA, Microsoft may transfer all personal data covered by the 2021 ILA as of the latest amendment to the United States or to any other country in which it or its sub-processors operate.[578]

334. In its reply to the preliminary assessment, the Commission states that:

> "*In view of the multitude of different constellations possible in the delivery of the technically complex services provided by Microsoft365, this level of detail provided in a framework contract is reasonable.*" [579]

The EDPS does not dispute the complexity of the services provided to the Commission in its use of Microsoft 365. However, in order to ensure proper compliance with the Regulation, and in particular to safeguard the rights of data subjects where their personal data are transferred to third countries, such complexity in fact inherently warrants a more detailed contractual specification related to transfers, not less detailed as suggested by the Commission. The fact that the contract governing processing in Commission's use of M365 is inter-institutional cannot justify any failure by the

[573] This includes transfers related to remoted access, customer-initiated transfers, protecting customers, directory data, network transit, service and platform quality and management and service-specific transfers. https://www.microsoft.com/licensing/terms/product/PrivacyandSecurityTerms/EAEAS. Website visited on 29 January 2024. See paras. 496 to 508 of this decision.

[574] The EDPS understands "system-generated data" as service generated data within the meaning of the 2021 ILA.

[575] Reply by Microsoft Ireland of 26 May 2023, Annex 7A, pp. 7, 10, See also https://learn.microsoft.com/en-us/privacy/eudb/eu-data-boundary-transfers-for-all-services.

[576] Commission's additional reply of 7 June 2022, Annex 1, p. 75.

[577] Under 2021 ILA (pp. 90 to 177), purposes for which sub-processors may process personal data (and for which such data may therefore be transferred to those sub-processors) include processing of personal data "*in the course of helping to provide*" or "*in the course of providing*" a specific Microsoft online service, without further specification.

[578] See clause 4(c) of the MBSA (2021 ILA p. 5), the section on "*Data Transfers*" in the body of the DPA (2021 ILA p. 38), the section on "*Data Transfers*" in the Software DPA Terms in Chapter 2 of Attachment 1 to the DPA (2021 ILA pp. 58-59), Chapter 3 of Attachment 1 to the DPA concerning standalone online services (2021 ILA pp. 62-64) and the section on "Data Transfers" in Chapter 4 of Attachment 1 to the DPA, concerning professional services (2021 ILA p. 67).

[579] Commission's reply of 25 May 2023, para. 109. See also paras. 13, 44 and 58 of the Commission's reply.

controller to comply with the Regulation, in particular as regards determination of the types of personal data and purposes of the processing. Nor can the inter-institutional nature of a contract allow for the requirements under the Regulation to be reduced or overlooked, thus lowering the protection of data subjects. In view of the allegations set out in the preliminary assessment, the Commission did not specify reasons as to why it considers the level of detail under the 2021 ILA reasonable given the technical complexity of the services provided to it.

Finding

335. It follows that the Commission has failed, both on the reference date and until the date of issuing this decision, to ensure that its contract with the processor sufficiently governs which types of personal data can be transferred to which recipient in which third country and for which purpose, and has failed to give Microsoft documented instructions in this regard. It has therefore infringed Article 29(3)(a) of the Regulation.

Deficiencies in the mapping of transfers by the Commission. Violation of Article 4(2), 46 and 48 of the Regulation

Transfer mapping by the reference date

336. Following the EDPS' order of 2 October 2020 (see paragraph 288), the Commission reported in a letter to the EDPS[580] high-risk transfers to the United States involving large-scale and complex processing. It reported that there were also other recipient non-EEA countries, namely: "*Where Microsoft has affiliates and identified sub-processors*".[581] This letter was not detailed, however; the material content of it amounted in essence to a single line in an Excel table describing many types of transfer. According to the Commission, it had completed a similar mapping exercise in September 2020.[582]

337. In its reply to the preliminary assessment, Microsoft Ireland suggests that the EDPS has never before required "*this level of granularity*" of transfer mapping and did not impose any specific level of granularity in the order of 2 October 2020.[583] In this regard, the EDPS stresses that the order of 2 October 2020 did not require that exhaustive information related to transfer mapping be reported to the EDPS as the order's objective was to promote compliance efforts of EUIs with the *Schrems II* judgment. Nor has the EDPS pronounced itself as to the compliance with that order by the Commission, and in particular granularity of the mapping, outside the context of present investigation. Moreover, the EDPS has not previously assessed, following the *Schrems II* judgment and in the context of an investigation, mapping of transfers related to the use by an EU institution or body of similarly complex services as those provided with Microsoft 365. In any event, the granularity of the information in the transfer mapping needs to be sufficient to enable the controller to 'master' its transfers so as to be able to achieve the objectives of Articles 46 and 48 of the Regulation as interpreted by the *Schrems II* judgment (*mutatis mutandis* as the Court of Justice was interpreting the GDPR). This is the level of granularity required by the applicable provisions.

---

[580] Commission's letter to the EDPS of 2 December 2020, Attachment 5, row 10 of the Excel table.
[581] Commission's letter to the EDPS of 2 December 2020, Attachment 5, column P of the Excel table.
[582] Commission's additional reply of 7 June 2022, p. 10.
[583] Reply by Microsoft Ireland of 26 May 2023, para. 224.

338. With regard to sub-processors, the Commission states that "*as provided by the ILA, such transfers take place only to the identified list of sub-processors"* and that *"the ILA goes even further to specify the location and the nature of the processing as well as the types and categories of personal data processed by each specific sub-processor*".[584]

339. The EDPS rejects these arguments. As recalled in paragraphs 325 and 333, under the 2021 ILA, Microsoft may transfer all personal data covered by the 2021 ILA to the United States or to any other country in which it or its sub-processors operate.[585] The Microsoft affiliates and sub-processors with access to the personal data processed on behalf of the Commission are listed in Attachment 4 to the DPA, which contains the "*Microsoft Online Services Sub-processors List*". This list only covers sub-processors involved in providing the online services. It does not cover sub-processors with access to data for the purposes of providing professional services, which are listed on a Microsoft website and subject to change. In addition, the information provided on the online services sub-processors does not always specify the jurisdictions from which those sub-processors have access to the personal data, but frequently only specifies where they are headquartered. Nor does it permit the Commission to distinguish which types of personal data are transferred where and for what purposes.

340. The EDPS requested confirmation of whether the international transfers associated with its use of Microsoft 365 began with the launch of the large-scale pilot.[586] The Commission has confirmed that:

> "*The occurrence of international transfers is not related to the number of users, meaning that transfers can be assumed to have taken place before the launch of the large-scale pilot*".[587]

This implies that the transfers started at the latest on 30 October 2019, when the first stage of the large-scale pilot was launched. This pre-dates the Commission's first transfer-mapping exercise, which was completed on 11 September 2020, and its transfer impact assessment, which was completed on 30 June 2021.

341. Prior to 16 July 2020, a valid adequacy decision was in place for transfers to the United States. However, this did not exempt the Commission from carrying out a transfer-mapping exercise, especially in relation to transfers to other third countries not benefitting from an adequacy decision. Without mapping its transfers, the Commission could not assess whether the transfers would be compliant with the purpose limitation and what measures were necessary to ensure their compliance with the Regulation. After the *Schrems II* judgment, which invalidated the adequacy decision benefitting the United States, a transfer-mapping exercise was all the more necessary. This is because the Commission could not comply with the requirements of the Regulation as interpreted by that judgment without having first carried out a complete transfer mapping.

---

[584] Commission' reply of 25 May 2023, para. 104.

[585] See clause 4(c) of the MBSA (2021 ILA p. 5), the section on "*Data Transfers*" in the body of the DPA (2021 ILA p. 38), the section on "*Data Transfers*" in the Software DPA Terms in Chapter 2 of Attachment 1 to the DPA (2021 ILA pp. 58-59), Chapter 3 of Attachment 1 to the DPA concerning standalone online services (2021 ILA pp. 62-64) and the section on "Data Transfers" in Chapter 4 of Attachment 1 to the DPA, concerning professional services (2021 ILA p. 67).

[586] EDPS letter to the Commission of 4 April 2022, p. 6.

[587] Commission's additional reply of 7 June 2022, p. 13.

342. In particular, the Commission could not comply with the requirements to assess whether any supplementary measures were required[588] and whether any effective supplementary measures existed and could be implemented to ensure an essentially equivalent protection of the transferred personal data.[589] As regards the United States, the Court of Justice itself concluded in the *Schrems II* judgment that the United States did not ensure an adequate (essentially equivalent) level of protection for personal data and that therefore supplementary measures were necessary with respect to transfers of personal data to that third country.[590] Without a complete transfer mapping, the Commission[591] could not make the assessments for other third countries to which personal data are transferred or are envisaged to be transferred under the 2021 ILA in the Commission's use of Microsoft 365. The Commission therefore could not ensure that the transfers of personal data in its use of Microsoft 365 are in compliance with the Regulation.

343. As noted in paragraphs 231 and 232, it is incumbent on a controller to appraise what data will be transferred where and for what purposes and to ensure their compliance prior to initiating a transfer. The Commission failed to do this. It has therefore infringed Articles 4(2), 46 and 48 of the Regulation.

Transfer mapping after the reference date

344. The 2021 DPIA contains a description of 11 potential transfer scenarios.[592] These transfer scenarios cover the collection of diagnostic and service generated data, synching of Azure Active Directory attributes, transfers of licensing and activation data sent by Microsoft 365 apps and access to personal data by Microsoft engineers outside the EEA to resolve support cases. Of these, the 2021 DPIA states that only four transfer scenarios effectively take place.[593] These four effective transfer scenarios entail transfers of service generated data to the United States, transfers related to the accessibility of M365 services from outside the EEA, transfers related to resolution of support cases by Microsoft engineers outside of the EEA and transfers of licensing and activation data.[594] The Commission has claimed that the remaining scenarios do not to entail actual

---

588 Steps 1-3 of the roadmap in EDPB Recommendations 01/2020.

589 Step 4 of the roadmap in EDPB Recommendations 01/2020.

590 See, to that effect, *Schrems II* judgment, in particular paras. 180 to 187.

591 As the controller responsible and accountable in line with Articles 4(2) and 26 of the Regulation for the processing, including transfers, that it carries out itself or others on its behalf.

592 Commission's 2021 DPIA, section 5.4.1, p. 91.

593 Commission's 2021 DPIA, section 5.4.1, p. 92. See also Commission's reply of 25 May 2023, para. 103.

594 A least some Azure Active Directory data (i.e. user ID and device ID) are transferred for the licensing verification purposes under transfer scenario T11 (Commission's 2021 DPIA, p. 92; see also Commission's reply of 25 May 2023, para. 103.4 and reply by Microsoft Ireland of 26 May 2023, Annex 12, p. 5). Microsoft's website confirms that it is Azure Active Directory data that are used (and thus transferred) as part of licensing checks: https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-licensing-whatis-azure-portal. According to Microsoft's website, Authentication and Licensing services are part of essential services for which required diagnostic and service data are "*collected and sent to Microsoft, regardless of any other privacy-related policy settings that you have configured. … Authentication is a cross-platform service that validates your Office user identity. It is required to enable you to sign in to Office, activate your Office license, access your files stored in the cloud, and provides a consistent experience across Office sessions and your devices. … Licensing is a cloud-based service that supports your Office activation for new installations and maintains the license on your devices after Office has been activated. It registers each of your devices and activates Office, checks the status of your Office subscription, and manages your product keys.*" See https://docs.microsoft.com/en-us/deployoffice/privacy/essential-services. Websites visited on 22 August and 20 December 2022, as well as on 30 January 2024.

transfers because certain data flows have been disabled by technical configuration[595] and because it has provisioned its tenant in the EU for the Microsoft products and services it uses.[596]

345. The EDPS analysed the Commission's description of effectively occurring transfers. The EDPS found that that description presented a number of discrepancies with other statements in the 2021 DPIA, with information available on Microsoft's website and accessorily with the results of the DPIAs conducted on behalf of the Dutch Ministry of Justice. The latter DPIA was conducted on certain products that are part of the Microsoft 365 software or its earlier versions, that concern flows of the same or similar types of data to Microsoft in the use of those products.

346. In view of those discrepancies concerning transfers, the EDPS addressed a number of requests for clarification and for further evidence to the Commission.[597] Those requests aimed to establish whether transfers were as limited as the Commission had concluded or broader in scope, and to establish what data were transferred to which locations and for what purposes. Our requests included a request for any data flow maps prepared by Microsoft or the Commission.

Transfers resulting from telemetry (diagnostic) data flows from Microsoft 365 apps, Teams client and OneDrive for Business

347. In the 2021 DPIA, the Commission concludes that no transfers of diagnostic data from Microsoft 365 Apps, Teams client and OneDrive for Business take place since this is disabled by technical configuration.[598]

348. In its request for further evidence,[599] the EDPS pointed out that the Dutch Ministry of Justice had concluded in its 2019 DPIA concerning Office 365 ProPlus that there was no technical configuration that would completely disable diagnostic data collection.[600] The EDPS also pointed to information in respect of the privacy controls for Microsoft 365 apps for enterprise[601] on Microsoft's website. Microsoft's website (covering privacy controls for various versions of Office products, including those supplied under Microsoft 365) states that even if administrators select the 'Neither' option, 'required service data' from users' devices continues to be sent to Microsoft via telemetry to help keep services "*secure, up-to-date and performing as expected*". The EDPS therefore pointed out to the Commission that it was unclear how such data differed from

---

595 Disabling by technical configuration as suggested by the 2021 DPIA refers to all diagnostic data flows to Microsoft from locally-installed software and optional connected experiences in Microsoft 365 Apps and Teams.

596 Commission's 2021 DPIA, section 5.4.1, p. 92.

597 EDPS letter to the Commission of 4 April 2022.

598 Commission's 2021 DPIA, see T2-T4, p. 92.

599 EDPS letter to the Commission of 4 April 2022.

600 The Dutch Ministry of Justice's DPIA of Office 365 ProPlus, 22 July 2019, pp. 8-9. Privacy controls provided by Microsoft allow administrators to set the level of diagnostic data sent to "Optional", "Required" or "Neither". The Dutch Ministry found that even when administrators set the level of diagnostic data to "Neither", Microsoft collects similar types of data as at the "Required" level. See also a similar finding by the Cypriot DPA in the EDPB report on the 2022 Coordinated enforcement action on the use of cloud-based services by the public sector, 17 January 2023, in particular in annex (p. 17).

601 See the second 'note' in a shaded box: https://docs.microsoft.com/en-us/deployoffice/privacy/overview-privacy-controls. See also https://docs.microsoft.com/en-us/deployoffice/privacy/required-service-data. Websites visited on 5 January, 30 March, 22 August and 20 December 2022 and 31 January 2024.

diagnostic data as this term was commonly understood and indicated that the Dutch Ministry of Justice's 2019 findings were still relevant.

349. These findings are also corroborated by information available on Microsoft's website, according to which Telemetry service is part of essential services for which required diagnostic and service data are "*collected and sent to Microsoft, regardless of any other privacy-related policy settings that you have configured. … The Telemetry service is used to collect diagnostic data from Office applications. It enables the collection of the diagnostic data generated by Office, both required and optional diagnostic data. It is also responsible for the collection of some required service data for Office.*"[602] These findings are also corroborated by information provided in the reply by Microsoft Ireland of 26 May 2023 to the preliminary assessment.[603]

350. In its request for further evidence, the EDPS also drew the Commission's attention to the Dutch Ministry of Justice's 2021 DPIA[604] in which they analysed telemetry events in captured network traffic concerning the individual use of Teams, Sharepoint and OneDrive.[605] That second DPIA found that Microsoft only documented and displayed 10% of telemetry data in its diagnostic data viewer, while 90% of detected telemetry events remained invisible in the viewer.[606] According to Microsoft's indication in that DPIA, the undocumented events were 'required service data'.[607] Microsoft explained to the Dutch Ministry of Justice that although it would not show these events in the diagnostic data viewer, it would provide them in response to a data subject access request.[608] That DPIA also found that even with the technical configuration set to disable the data collection,[609] OneDrive allowed the collection of 'required service data' containing directly identifying personal data (readable usernames, file path or email address).[610] These findings of the DPIA of the Dutch Ministry of Justice are also

---

[602] See https://docs.microsoft.com/en-us/deployoffice/privacy/essential-services. Website visited on 22 August and 20 December 2022, as well as on 31 January 2024.

[603] See, in this respect, reply by Microsoft Ireland of 26 May 2023, Annex 5, paras. 94 and 98, Annex 12 (Microsoft 365 Major Services Data Flows), and Annex 14 (Overview of privacy controls for Microsoft 365 Apps for enterprise, dated 27 March 2023). See also para. 307 of this decision.

[604] The Dutch Ministry of Justice's DPIA on Microsoft Teams, OneDrive, Sharepoint and Azure AD, 16 February 2022.

[605] The Dutch Ministry of Justice's DPIA on Microsoft Teams, OneDrive, Sharepoint and Azure AD explains on p. 10: "*Technically, Microsoft collects Diagnostic Data in different ways, via system-generated event logs on its own cloud servers and via the telemetry clients in the different clients and through the browser. Similar to the telemetry client in Windows 10 and in Office 365 ProPlus, Microsoft has programmed the mobile Office apps and Office for the Web to systematically collect Telemetry Data on the device, and regularly send these to Microsoft's servers in the USA. Additionally, Microsoft creates detailed Analytics & reports about individual use of Teams.*". On p. 93, that DPIA also explains: "*Microsoft can continuously collect new types of Diagnostic Data, both on its own cloud servers and through the telemetry clients built into the Teams, OneDrive and Sharepoint applications on the different platforms (where available). Therefore, any analysis of the Diagnostic Data remains a snapshot. Data processing remains dynamic.*" See similarly the Dutch Ministry of Justice's DPIA on Office 365 ProPlus, 22 July 2019, pp. 18, 14 and 32).

[606] The Dutch Ministry of Justice's DPIA on Microsoft Teams, OneDrive, Sharepoint and Azure AD, pp. 26-27.

[607] The Dutch Ministry of Justice's DPIA on Microsoft Teams, OneDrive, Sharepoint and Azure AD, p. 27.

[608] The Dutch Ministry of Justice's DPIA on Microsoft Teams, OneDrive, Sharepoint and Azure AD, p. 27.

[609] Meaning that diagnostic data collection is set to 'Neither'.

[610] The Dutch Ministry of Justice's DPIA on Microsoft Teams, OneDrive, Sharepoint and Azure AD, 16 February 2022, pp. 5 and 30.

corroborated by information available on Microsoft's website.[611] There is no indication in the Commission's 2021 DPIA that it was aware of this data collection.[612]

351. The EDPS asked the Commission to clarify what personal data Microsoft collects by telemetry from the Microsoft 365 applications used by the Commission, including Teams and OneDrive for Business; for what purposes; whether those data are transferred out of the EEA and where they are stored.[613]

352. In its reply to the request for further evidence, the Commission has acknowledged that some telemetry data flows do occur despite its adjusted configuration of Microsoft 365 software. This is because the Commission makes use of certain "*connected experiences*" provided by Microsoft.[614] In the Commission's stated view, these require the collection of usage and performance data and metadata.[615] The Commission has informed the EDPS that these data are transferred to the United States and are stored there.[616] It has therefore identified a new effective transfer scenario that was not listed in its 2021 DPIA. The new effective transfer scenario is "*processor connected experiences in Microsoft 365 Enterprise Apps*". In relation to this scenario, the Commission has stated that only the diagnostic data part of required service data is transferred to the United States, while the customer data part is stored in the EU. The Commission has further stated that in another potential transfer scenario ("*controller connected experiences in Microsoft 365 Enterprise Apps*"), there are no effective transfers since the related functionality is disabled by technical configuration and therefore unavailable to Commission users.[617]

353. It follows that at the time it completed the 2021 DPIA, the Commission did not have a sufficiently clear understanding of which personal data were transferred to which recipients in which third countries.[618] Moreover, in its reply to the preliminary assessment, the Commission states that: "*the technical aspects of [...] data flows [related to the use of processor connected experiences] will be further investigated and regulated in future versions of the DPA*".[619] In the EDPS' view, this statement demonstrates that at least by 25 May 2023, the Commission still did not fully comprehend those data flows. The statement also suggests that the Commission recognises that the data flows should be regulated in a contract under Article 29(3) of the Regulation.

---

[611] See https://docs.microsoft.com/en-us/deployoffice/privacy/overview-privacy-controls. See also https://docs.microsoft.com/en-us/deployoffice/privacy/required-service-data and https://learn.microsoft.com/en-us/microsoftteams/policy-control-overview. Websites visited on 5 January, 30 March, 22 August and 20 December 2022 and 31 January 2024.

[612] See also Commission's additional reply of 7 June 2022, p. 6.

[613] EDPS letter to the Commission of 4 April 2022.

[614] Commission's additional reply of 7 June 2022, pp. 5 and 6. The transfers in the new transfer scenario 12 concern required services data when the Commission uses what it calls "*processor connected experiences*" in Microsoft 365 Enterprise Apps.

[615] Commission's additional reply of 7 June 2022, p. 5.

[616] Commission's additional reply of 7 June 2022, p. 5.

[617] Commission's additional reply of 7 June 2022, pp. 5 and 6 (transfer scenarios T12 and T13).

[618] Commission's additional reply of 7 June 2022, p. 6.

[619] Commission's reply of 25 May 2023, para. 125. The Commission similarly states in para. 135 of its reply that it "*has entered into exchanges with Microsoft on [the] reports [issued by the Dutch Government and the Supervisory Authority of Baden-Württemberg, Germany, which indicate that data transfers of Diagnostic Data from the controller to Microsoft Corp. would take place]*" and that it "*will carry out own investigations to gain further clarity*".

354. The Commission's reply has also acknowledged that as part of the required service data Microsoft collects directly identifying personal data from OneDrive for Business.[620] It stated, however, that these required service data flows remain inside the "*trusted O365 compliance boundary*".[621] The EDPS understands this to be a reference to the 'EU Data Boundary' implemented by Microsoft.[622] As explained in paragraphs 330, 331 and 496 to 508, transfers continue despite the implementation of the EU Data Boundary for, among others, support and security purposes. Since, as stated on Microsoft's website, required service data are necessary to keep the underlying service "*secure, up to date and performing as expected*",[623] they can be transferred outside of the EEA and therefore those data are not included in the EU Data Boundary. In their reply to the preliminary assessment, neither the Commission nor Microsoft Ireland have specifically disputed this conclusion, nor have they presented any evidence disputing it. The EDPS therefore considers that the Commission has not obtained any guarantees that these required service data will remain in the EEA.

Service generated data

355. The 2021 DPIA suggests that service generated data in the context of its use of Microsoft 365 are only sent to the United States.[624] The 2021 DPIA does not explain how the Commission may have reached this conclusion.

356. Microsoft has confirmed that the instructions set out in the 2021 ILA[625] allow Microsoft "*to transfer such data to any country in which [it] or its Sub-processors operate*".[626] It has added that: "***most*** *of [the service generated data] are currently transferred and processed in the United States*" (emphasis added).[627] The EDPS understands that statements such as this have informed the Commission's opinion of where service generated data are transferred. However, Microsoft's statement that "*most*" of these data are transferred to the United States suggests that some service generated data may be transferred to other third countries.[628]

357. In June 2022, the Commission has communicated that:

> "*there are still no publicly available resources detailing all [service generated data] flows. Microsoft is reportedly working on detailed documentation and anticipates having these available in the Q3 2022 timeframe*".[629]

---

620 Commission's additional reply of 7 June 2022, p. 6.
621 Commission's additional reply of 7 June 2022, p. 6.
622 Reply by Microsoft Ireland of 26 May 2023, Annex 7A.
623 See https://docs.microsoft.com/en-us/deployoffice/privacy/required-service-data, https://learn.microsoft.com/en-us/azure/active-directory/fundamentals/azure-ad-data-residency and https://docs.microsoft.com/en-us/deployoffice/privacy/overview-privacy-controls. Websites visited on 5 January, 30 March 2022, 22 August and 20 December 2022 and 31 January 2024.
624 Commission's 2021 DPIA, section 3.6, p. 28, section 3.6.9, p. 42, and section 5.4.1, pp. 91 and 92.
625 2021 ILA, p. 58.
626 Microsoft letter to the Commission of 2 June 2022, p. 6 (Annex 5 to the Commission's additional reply of 7 June 2022). See also reply by Microsoft Ireland of 26 May 2023, Annex 5, para. 103, as well as paras. 101 and 125.
627 Microsoft letter to the Commission of 2 June 2022.
628 See in this respect also reply by Microsoft Ireland of 26 May 2023, Annex 5, para. 101, and Annex 12.
629 Commission's additional reply of 7 June 2022, p. 7. See similar statement regarding required service data on p. 8.

This further suggests that at the time it completed its 2021 DPIA and beyond,[630] the Commission did not have a clear and detailed understanding of the data flows resulting from its use of Microsoft 365. Nor did Microsoft appear to have such understanding. In its reply to the preliminary assessment, Microsoft Ireland has provided a document entitled "Microsoft 365 Major Services Data Flows" which was last updated on 25 August 2021.[631] The Data Flows document therefore pre-dates the Commission's reply of June 2022 in which the Commission acknowledges that Microsoft is still working on detailed documentation setting out all service generated data flows. It follows that the Data Flows document may not include all service generated data flows. See, in this respect, also the EDPS' analysis in paragraphs 331 to 334 and 496 to 508 of this decision in which the EDPS finds, in particular, that the numerous exceptions to and exclusions from the EU Data Boundary, which cover customer data, service generated data, diagnostic data and professional services data,[632] demonstrate that transfers of personal data related to the Commission's use of Microsoft 365 outside the EEA continue to a significant extent.

Level of granularity in mapping transfers

358. In its reply to the preliminary assessment, Microsoft Ireland states that no "*specific level of granularity*" is legally required.[633] In this regard, the EDPS refers to paragraphs 231 to 236 of this decision. While the mapping of the transfers does not need to be detailed down to individual datasets, the types of personal data transferred should be known to the controller for it to be able to assess the measures necessary (or not) to ensure the continuity of their protection once transferred. The complexity of the services provided and the need to foresee evolutions of the software services provided cannot result in exempting the controller from fulfilling its obligations to the (minimum) level required by the applicable rules for these rules to achieve their purpose, which is to protect the personal data of the natural persons concerned. Moreover, the EDPS considers that Microsoft Ireland has not demonstrated how the level of transfer mapping carried out by the Commission as described above is sufficient to ensure compliance with Articles 46 and 48 of the Regulation. Nor has the Commission as the controller done so.

359. In this regard, Microsoft Ireland further states that:

> "*it is not reasonable to expect contractual parties to map out transfer details in an overly detailed manner – this stifles provision of the services, creates an undue cybersecurity and business secrets risk, and would in practice require the parties to constantly update the contract and transfer mapping descriptions (for instance, when a certain feature is or is not turned off by the Commission or the user)*".[634]

The EDPS considers that in this statement Microsoft Ireland fails to substantiate what it considers to be an "*overly detailed manner*" of mapping the transfers. The EDPS rejects that, as alluded to by Microsoft Ireland, it is not necessary for the Commission to know whether a certain feature is turned off or not, when this has direct implications on the scope[635] and nature of the transfers of personal data. The EDPS also rejects that the requirements in this regard, as interpreted above, are not proportionate, as suggested

[630] The quoted statement was made on 7 June 2022 when the Commission provided its additional reply.
[631] Reply by Microsoft Ireland of 26 May 2023, Annex 12.
[632] Reply by Microsoft Ireland of 26 May 2023, Annex 7A, pp. 7, 10, See also https://learn.microsoft.com/en-us/privacy/eudb/eu-data-boundary-transfers-for-all-services.
[633] Reply by Microsoft Ireland of 26 May 2023, paras. 224 and 231.
[634] Reply by Microsoft Ireland of 26 May 2023, para. 225.
[635] In particular which types of personal data are transferred.

by Microsoft Ireland. In particular, the EDPS considers that there should be a minimum level of awareness of the types of personal data transferred by the controller, such as to allow this latter to make sure that the level of protection is ensured in relation to such types. Ignorance as to entire types of personal data being transferred does not allow the controller to discharge its obligations. Furthermore, Microsoft Ireland has not specifically substantiated the insinuated disproportionality of the requirement to carry out a proper mapping of the transfers. Such mapping is vital to ensuring an essentially equivalent level of protection with regard to the transferred personal data and is proportionate given the complexity of the services provided and the transfers involved.

Findings

360. The Commission has been unable to provide the EDPS with more than broad and generic descriptions of what personal data are transferred outside the EEA. Most importantly, such descriptions are incomplete, as demonstrated in particular in section 3.1.2.1 and paragraphs 314 to 359 of this decision. In June 2022, the Commission confirmed that detailed data flow maps were still in preparation by Microsoft.[636]

361. The EDPS has since received data flow overviews that pre-date June 2022[637] or are not complete.[638] The Commission has also been unable to provide detailed information on the changes to data flows after the implementation of EU Data Boundary. In its reply to the preliminary assessment, Microsoft Ireland has provided certain information on data flows outside the EEA,[639] some of which pre-dates June 2022.[640] That information is, however, not sufficiently complete to allow the Commission to understand which types of personal data are transferred to which third countries. The information contains general descriptions, only referring to selected examples, and, crucially, not listing all data flows that result in transfers outside of the EEA. The information is also not specific to the Commission's use of Microsoft 365. Moreover, the amendment to the DPA of 19 December 2023 in so far as it pertains to EU Data Boundary does not clearly delineate which types of personal data are covered, as explained in paragraphs 331 to 334 of this decision.

362. It follows that the Commission has not demonstrated to possess the minimum level of understanding of the data flows resulting from the 2021 ILA in the Commission's use of Microsoft 365, nor of the associated transfers to third countries, required to comply with Articles 46 and 48 of the Regulation.

363. By not knowing exactly what transfers it allows, the Commission as a controller has failed to obtain the minimum information necessary to start determining whether any supplementary measures are required to ensure an essentially equivalent level of protection and whether any effective supplementary measures exist and could be implemented.[641] It failed to obtain this information prior to initiating the transfers and prior to completing its October 2021 transfer impact assessment. Moreover, the EDPS

---

636 Commission's additional reply of 7 June 2022, p. 9.
637 Reply by Microsoft Ireland of 26 May 2023, Annex 12.
638 Cf. Commission's reply of 25 May 2023, para. 125.
639 Reply by Microsoft Ireland of 26 May 2023, Annexes 2, 5, 6, 7.A, 7.B and 12.
640 Reply by Microsoft Ireland of 26 May 2023, Annex 12. That document was last updated on 25 August 2021.
641 See in this respect also the EDPB report on the 2022 Coordinated enforcement action on the use of cloud-based services by the public sector, 17 January 2023, in report (pp. 17, 20 and 31) and annex (pp. 52 to 55, 77, 78, 87 to 89, 100 to 102, 105, 106, 110, 125 and 126).

could not obtain such information since, despite reiterated requests.[642] The Commission has therefore failed to provide appropriate safeguards ensuring that data transferred enjoy an essentially equivalent level of protection to that of the EEA, and it has therefore infringed Articles 4(2), 46 and 48 of the Regulation.

Assessment of compliance with the specific purpose limitation for transfers under the Regulation (Article 47(1))

364. In order to allow transfers, the Commission must ensure that they take place "*solely to allow tasks within the competence of the controller to be carried out*", as required by Article 47(1) in light of Articles 4, 5, 6, 9 and 46 of the Regulation.[643] As explained in paragraph 247, without applying this specific limitation of purposes also to transfers subject to appropriate safeguards under Article 48 of the Regulation, and not just to transfers covered by adequacy decisions, the continuity of the protection for personal data transferred cannot be ensured. It is therefore incumbent on the Commission to limit the purposes for which personal data are transferred out of the EEA by the Commission or by Microsoft on its behalf, to purposes without which the Commission cannot carry out its tasks.

365. In its reply to the preliminary assessment, the Commission states that there is no infringement of Article 47(1) of the Regulation because:

> *"the transfers taking place under the DPA are necessary for the functioning and management of the Commission, particularly by enabling Microsoft365 as business-critical IT operation of the Commission, and are therefore carried out in the public interest for the proper performance of tasks within the Commission's competence."*[644]

The Commission further states that:

> "*transfers only take place* ***to enable the provision of the service****, which in turn is necessary for the Commission to perform its functions and mandate. From this, it follows that data is only transferred in the public interest, particularly to allow for the management and functioning of the Commission.*" (emphasis added)[645]

The EDPS does not concur with those statements, as demonstrated in the following paragraphs. In addition to that, the EDPS stresses that the 2021 ILA clearly envisages processing for Microsoft's business purposes and does not exclude transfers for such purposes. Moreover, as the Commission itself acknowledges,[646] Annex I.B to the processor to processor SCCs for transfers between Microsoft Ireland and Microsoft Corporation includes "*business operations incident to providing the products and services*" among permitted purposes of transfers.

366. As shown in section 3.1.2, the 2021 ILA's purpose limitations retain similar deficiencies to those identified in the EDPS' 2020 Findings and Recommendations. In particular, the

---

[642] EDPS' requests of 12 May 2021 and 4 April 2022 in the present investigation, as well as EDPS' recommendations from its 2019-2020 investigation (in particular recommendations 15, 23 and 31), and EDPS' order of 2 October 2020.

[643] Article 47(1) of the Regulation, read in the light of Articles 4, 5, 6, 9 and 46.

[644] Commission's reply of 25 May 2023, para. 98.

[645] Commission's reply of 25 May 2023, para. 128.

[646] Commission's reply of 25 May 2023, para. 106.

purposes for which personal data are collected under the 2021 ILA are not sufficiently explicit and specified, as required by the Regulation.[647]

367. Moreover, as shown in paragraphs 315 to 335, the contractual right by the Commission to control the storage location of the personal data under the EU Storage Guarantee and the EU Data Boundary is limited in scope. There are no clear instructions in the 2021 ILA on the purposes for which personal data that are not covered by the EU Storage Guarantee or EU Data Boundary may be transferred.[648] Moreover, the transfers that take place in practice largely serve Microsoft's own business purposes and compensate for limitations in Microsoft's ability to provide services from within the EEA.

368. The EDPS considers that the Commission also does not have clear non-contractual information on what types of personal data are transferred for which purposes (see paragraphs 339 to 362).[649]

369. The Commission is therefore not equipped to determine whether specific transfers are occurring "*solely to allow tasks within the competence of the controller to be carried out*". Nonetheless, the EDPS has assessed whether the transfers would comply with this specific purpose limitation in view of the purposes of processing under the 2021 ILA, as follows.

370. Processing for the purposes of "*improving the core functionality of accessibility, privacy or energy efficiency*", "*compliance with legal obligations*" as well as "*combatting fraud, cybercrime and cyberattacks*"[650] were included in the business operations purposes under the 2021 ILA until 19 December 2023.[651] However, as explained in paragraph 179, the EDPS considers that, both prior and after the conclusion of the amendment of 19 December 2023,[652] the DPA implicitly includes these three purposes within the description of the "*Processing to Provide Customer the Online Service*". The EDPS considers that these three purposes could be deemed necessary for the Commission to carry out its tasks in so far as the processing for those purposes is carried out to comply with an obligation under EU or Member State law, in compliance with the data minimisation principle.[653]

---

[647] See in this respect similarly the findings of the Conference of German DPAs on Microsoft Online Services (Microsoft 365), 24 November 2022, in summary (pp. 3, 4) and assessment (p. 54).

[648] See paras. 323, 325, 328, 332 and 333 of this decision.

[649] In light of information provided in the 2021 DPIA and in Commission's additional reply of 7 June 2022, as well as written and oral replies by the Commission and by Microsoft Ireland to the preliminary assessment. See in this respect similarly the findings of the Conference of German DPAs on Microsoft Online Services (Microsoft 365), 24 November 2022, in summary (pp. 3, 4) and assessment (pp. 7 to 11, 13 to 14, 54).

[650] As regards "*combatting fraud, cybercrime and cyberattacks*" this would include legal obligations to ensure the security and confidentiality of information (see 2020 Findings and Recommendations, pp. 26-27).

[651] See paras. 175, 178 and 179 of this decision.

[652] See para. 86 of this decision for how the 2021 ILA prior to the amendment of 19 December 2023 defines providing an online and professional service. The amendment of 19 December 2023 has modified the description of "to provide" an online service only by stipulating that "ongoing improvement" is limited to the online service that the customer uses or subscribes to.

[653] Neither Microsoft Ireland nor any other sub-processor in the EU may provide the services the Commission needs without complying with EU or Member State law. The EDPS points out that the processing must be strictly necessary for compliance with a legal obligation to which Microsoft Ireland and any other sub-processor in the EU is subject, pursuant to a provision of EU law or the law of the Member State concerned, where that legal basis meets an objective of public interest and is proportionate to the legitimate aim pursued and where that processing is carried out only in so far as is strictly necessary. See, in this respect, Article 5(2) of the Regulation, Article 6(3) GDPR and judgment in case C-252/21, *Meta Platforms and Others*

371. Some of the processing falling within Microsoft's business purposes following the amendment of 19 December 2023[654] could be considered necessary for the Commission to carry out its tasks. In the context of the "*billing and account management*" business purpose, this could be the case for processing of basic billing and account data to obtain payment from the Commission.[655] Processing for the purposes of "*financial reporting*" as one of the four remaining business operations purposes also entails complying with the "*applicable laws and regulations*", as stated by Microsoft Ireland.[656]

372. However, other processing operations appear to be of interest only to Microsoft and are clearly not necessary for the Commission to carry out its tasks. As set out in section 3.1.2.3, the 2021 ILA permits Microsoft to process personal data for the purposes of its product strategy, its relationship with its employees and partners, the management of its business relationship with its customers, internal reporting, forecasting and business modelling.[657] These purposes are not indispensable to providing the services that the Commission requires to carry out its tasks.[658]

373. Processing for Microsoft's business purposes is distinct from its ongoing improvement of the services, which forms part of how the 2021 ILA defines the provision of the services procured under it.[659] It could be considered necessary for the Commission's performance of its tasks to allow some processing for the purposes of monitoring the Commission's use of Microsoft's products and services with a view to improving them.[660] However, the scope and nature of processing for improvement of the services that the Commission subscribes to needs to be clearly defined in a contract or another binding legal act under EU or Member State law.[661] As demonstrated in paragraphs 90 to 97, the Commission has failed to specify the purposes of ongoing improvement as required by Articles 4(1)(b) and 29(3) of the Regulation. Moreover, such processing would need to observe strictly the principles of data minimisation, transparency and proportionality.[662] The Commission would also need to ensure that appropriate technical and organisational measures and safeguards for such processing are put in place.[663]

374. As explained in paragraphs 98 to 105, the 2021 ILA is not clear whether providing a particular online or professional service includes only "troubleshooting" in respect of that service or whether it includes troubleshooting in respect of other or all online or

---

(Conditions générales d'utilisation d'un réseau social), ECLI:EU:C:2023:537, paras. 127, 128, 132, 138 and 139, judgment in case C-184/20, *Vyriausioji tarnybinės etikos komisija*, ECLI:EU:C:2022:601, para. 85, and judgment in case C-175/20, *Valsts ieņēmumu dienests (Processing of personal data for tax purposes)*, EU:C:2022:124, para. 83. As the controller for processing for its business operations, and therefore the designer of the processing operations concerned, it is for Microsoft, in accordance with the principle of accountability laid down in Article 5(2) of the GDPR, to demonstrate that the processing is carried out for that purpose and, where appropriate, that the processing is in accordance with the objective of the collection of the data. See, to that effect, opinion of Advocate General Pikamäe in Case C-77/21, Digi, ECLI:EU:C:2022:248, points 46 and 47.

654 See paras. 175, 177 and 178 of this decision.

655 See para. 190 of this decision.

656 Reply by Microsoft Ireland of 26 May 2023, Annex 4, p. 15.

657 See para. 177 of this decision.

658 See also para. 196 of this decision as to why the processing for business purposes is not incidental to the provision of services to the Commission. See also paras. 186 to 195 and 197 to 199 of this decision establishing Microsoft's controllership for the processing for business purposes.

659 2021 ILA, section on "Processing to Provide Customer the Online Services", p. 28.

660 See 2020 Findings and Recommendations, pp. 26-27.

661 In accordance with Articles 26, 29 and 30 of the Regulation.

662 In accordance with Articles 4 and 27 of the Regulation.

663 In accordance with Articles 26, 27, 29, 33, 36 and Chapter V of the Regulation.

professional services respectively. In fact, as explained in paragraphs 100 and 101, it follows from Microsoft's letter cited by the Commission that Microsoft can process personal data under the 2021 ILA to troubleshoot online services that are not provided to the Commission. This means that personal data are not only transferred for troubleshooting related to the Commission's services[664] but are also intended for processing, after the transfer, for the purpose of improving services that the Commission does not subscribe to. In accordance with Articles 46 and 47(1) of the Regulation these transfers cannot be considered as taking place solely to allow the Commission's performance of tasks within its competence. As provided in the 2021 DPIA, transfers take place in relation to resolution of support cases by Microsoft engineers outside of the EEA.[665] Based on the information provided by Microsoft Ireland,[666] the EDPS further understands that such transfers are continuing following the implementation of the EU Data Boundary.[667] Such transfers are therefore a further instance of transfers taking place for purposes that are broader than are permitted under Article 47(1) of the Regulation.

375. In view of the above, the EDPS rejects the assertion by Microsoft Ireland that the EDPS has not demonstrated that the Commission has failed to satisfy the purpose limitation provided for in Article 47(1) of the Regulation. [668]

Finding

376. The Commission has therefore failed, on the reference date and until the date of issuing this decision, to ensure that transfers take place "*solely to allow tasks within the competence of the controller to be carried out*." This is in breach of Article 47(1) of the Regulation, read in the light of Articles 4, 5, 6, 9 and 46.

Commission's transfer impact assessment in the 2021 DPIA completed after the signature of 2021 ILA

377. As noted in paragraphs 260 to 271, in order to allow transfers envisaged under the 2021 ILA, the Commission as the controller must first ensure that the transfers take place only where an essentially equivalent level of protection is guaranteed as in the EEA by the Regulation, read in light of the Charter, or that, in the alternative, the transfers can take place under the provisions on derogations where the conditions to have recourse to such a transfer tool are met. In the absence of an adequacy decision, the Commission must therefore carry out a transfer impact assessment to assess the level of protection in the context of the specific transfers.

378. EDPB Recommendations 01/2020 clarify how to fulfil the requirements stemming from EU data protection law in light of the *Schrems II* judgment to ensure that transferred personal data enjoy a level of protection essentially equivalent to that guaranteed in the EEA, and EDPB Recommendations 02/2020 specifically clarify the European Essential

[664] Commission's 2021 DPIA, section 5.4.1, p. 91. See also Commission's reply of 25 May 2023, para. 103.
[665] Commission's 2021 DPIA, section 5.4.1, p. 91. See also Commission's reply of 25 May 2023, para. 103.
[666] See reply by Microsoft Ireland of 26 May 2023, Annex 7.A, p. 7, and Annex 7.B, pp. 9-11, 13, 15., as well as https://www.microsoft.com/licensing/terms/product/PrivacyandSecurityTerms/EAEAS (Product Terms site).
[667] Reply by Microsoft Ireland of 26 May 2023, Annex 7A, p. 7, and Product Terms site, https://www.microsoft.com/licensing/terms/product/PrivacyandSecurityTerms/EAEAS.
[668] Reply by Microsoft Ireland of 26 May 2023, para 265.

Guarantees for surveillance measures. The EU institutions and bodies should therefore take those recommendations into account when performing their transfer impact assessments.

379. In accordance with the *Schrems II* judgment,[669] supplementary measures will be required where problematic legislation or practices[670] in the third country, such as relating to access by public authorities of that third country to transferred data, prevent an essentially equivalent level of protection, as guaranteed by appropriate safeguards under the transfer tool provided in Article 48 of the Regulation, from being afforded to the transferred personal data.[671]

380. As noted in paragraph 265, public authorities in third countries may endeavour to, actively or passively, access transferred personal data while the data are in transit to the intended recipient or while the data are in custody by the intended recipient.[672]

381. It follows that where the Commission envisages using 'appropriate safeguards' as a transfer tool, such as standard or *ad hoc* contractual clauses for transfers, it must implement effective supplementary measures, if they are required, in order to be able to allow transfers.[673]

382. In addition to transfers to the United States, the 2021 ILA foresees several other transfer destinations. Indeed, in addition to recipients in the United States, Attachment 4 to the DPA lists 75 envisaged transfer recipients, which are contractually permitted to process personal data[674] and are located in third countries that are covered by an adequacy decision and in third countries that are not covered: Australia, Brazil, Canada, Chile, China, Egypt, Hong Kong, India, Israel, Japan, Malaysia, Republic of Korea, Serbia, Singapore, South Africa, Switzerland, the United Arab Emirates and the United Kingdom.

383. With respect to the 2021 ILA, the Commission was therefore required to conduct a transfer impact assessment in respect of each recipient in a destination not covered by an adequacy decision before it signed the 2021 ILA.[675]

384. The Commission's 2021 DPIA, which was completed on 15 October 2021[676] after the signature of the 2021 ILA on 7 May 2021,[677] contains a chapter entitled 'Transfer Impact Assessments' focusing on certain transfers to the United States.[678] The 2021 DPIA does not specifically explain on what basis the Commission ruled out the possibility of transfers, including onward transfers, occurring to destinations other than the United States. The EDPS considers such an explanation to be necessary in light of the

669 See *Schrems II* judgment, paras. 131-134.
670 See para. 264 of this decision.
671 Articles 46 and 48 of the Regulation as interpreted in light of the Charter. See also EDPB Recommendations 01/2020, paras. 22 and 23.
672 EDPB Recommendations 01/2020, para. 80.
673 See *Schrems II* judgment, paras. 131-134, and EDPB Recommendations 01/2020, paras. 22 and 23.
674 See 2021 ILA, pp. 89 to 177. See also reply by Microsoft Ireland of 26 May 2023, Annex 1.C (list of sub-processors as last updated on 18 November 2021).
675 I.e. Australia, Brazil, Chile, China, Egypt, Hong Kong, India, Malaysia, Serbia, Singapore, South Africa, the United Arab Emirates and, prior to the entry into force of the adequacy decision adopted on 10 July 2023, the United States.
676 See para. 297 of this decision.
677 See para. 292 of this decision.
678 Commission's 2021 DPIA, pp. 86 to 100.

contractual permission that the Commission has granted Microsoft to transfer personal data to any country in which Microsoft, its affiliates and sub-processors operate, and given the global nature of Microsoft's infrastructure and resources.[679]

385. For example, the 'follow the sun' support model for critical incidents implies transfers to potentially any destination envisaged under the 2021 ILA, in particular to India, given its pre-eminent place in the global IT support-service industry. Thus, and purely as an example, the EDPS would have expected the Commission to have included transfers to, and remote access from, at least India in its transfer impact assessment. At the very least, it should have been explained why, despite the Commission benefitting from the 'follow the sun' support model, such a transfer impact assessment was unnecessary.

386. The only transfer destination assessed by the Commission in the 2021 DPIA was the United States. In that assessment, the Commission concluded that supplementary measures were required due to the surveillance practices permitted by 50 USC § 1881a (section 702 FISA).[680] However, the EDPS notes that in its transfer impact assessment, the Commission did not accurately assess the United States law with regard to the required supplementary measures. In particular, the Commission stated in its 2021 DPIA that: "*Microsoft is not under any specific legal obligation to decrypt any information prior to its disclosure to the US authorities.*"[681] The Commission did not, however, assess, as it should have, whether Microsoft was under a legal obligation to hand over the encryption keys which would allow the US authorities to decrypt the data themselves.

387. Had the Commission carried out a proper transfer impact assessment with regard to the United States, and in particular had it made a complete assessment of relevant US law, it would have found that US law in fact does impose a legal obligation requiring entities under US jurisdiction to hand over encryption keys which allow US authorities to decrypt data.[682] As further explained below in the assessment of the implemented supplementary measures, the Commission wrongly concluded on the basis of this incomplete assessment that Microsoft's encryption solutions protected personal data from disclosure requests made under US law.[683]

388. Moreover, the results of its transfer impact assessment would only have been complete had the Commission assessed the level of protection afforded by other recipients and transfer destinations permitted under the 2021 ILA. For certain countries - such as countries in respect of which an adequacy decision is due to be issued[684] - a transfer impact assessment might show that the Commission could rely on contractual measures, without supplementary measures, to ensure appropriate safeguards for

---

679 2021 ILA, p. 58. See also reply by Microsoft Ireland of 26 May 2026, para. 253, in which it acknowledges that Microsoft works with external parties which are located in countries such as China and India. It states that Microsoft provides onward transfer SCCs for transfers to such external parties.

680 Commission's 2021 DPIA, p. 95.

681 Commission's 2021 DPIA, p. 96.

682 In addition to the Court's assessment in the *Schrems II* judgment, see Ian Brown and Douwe Korff, Exchanges of Personal Data After the Schrems II Judgment, July 2021; Stephen Vladeck, Expert Opinion on the Current State of U.S. Surveillance Law and Authorities, commissioned by the Conference of German DPAs; the Rapport sur l'US CLOUD Act from the Federal department of justice and police of the Swiss Confederation; the Memorandum on the Application of the CLOUD Act to EU Entities commissioned by the Dutch Ministry of Justice and Security (NCSC); or the sources listed in EDPB Recommendations 01/2020 at footnote 60, p. 21.

683 Commission's 2021 DPIA, p. 96.

684 Where the Commission has already issued a proposal for an adequacy decision and the EDPB has issued or is about to issue a positive opinion.

transfers to recipients in those countries.[685] That might be the case for e.g. Brazil.[686] However, a transfer impact assessment would likely lead to a different outcome for certain other countries, such as China, India,[687] and the United Arab Emirates.[688] It therefore cannot be excluded, and actually it is quite probable, that those countries have legislation and governmental practices that are liable to prevent compliance by the recipients with the binding commitments made to the Commission in the 2021 ILA and therefore to prevent compliance by the Commission with the Regulation.

389. Where the foregoing assessment had showed that supplementary measures were required, the Commission should have proceeded to the assessment as to whether it was even possible to implement effective supplementary measures.

390. The EDPS takes note that Microsoft Ireland states that:

> *"Microsoft has assessed the publicly available information related to the laws and practices of destination countries outside the EU, EEA, and countries whose laws and practices are deemed adequate by the European Commission, along with safeguards put in place by Microsoft. Based on this assessment, Microsoft believes these laws and practices do not in practice prevent it from fulfilling its obligations under the SCC in regard to transfers of personal data outside the EU and they are compatible with the requirements of GDPR Article 46.* [689]
>
> *[B]efore opening (or considering opening) a data center in a new country, Microsoft conducts a rigorous assessment of local laws to validate that data in the country will be hosted in a manner that is consistent with Microsoft obligations to its customers.*"[690]

The EDPS notes, however, that Microsoft Ireland has not submitted any evidence demonstrating the performance of such an assessment with regard to third countries not covered by an adequacy decision.[691] Microsoft Ireland also has not specified what such an assessment entailed. It follows that any reliance by the Commission on the assessment carried out by Microsoft Ireland of the third-country legislation and

---

685 See para. 126 of the *Schrems II* judgment.

686 Information on the legislation and practices Information on the legislation and practices in Mexico, Türkiye and Brazil can be found e.g. in the legal studies "Government access to data in third countries - Mexico and Turkey" and "Government access to data in third countries – Brazil", commissioned by the EDPB.

687 Information on the legislation and practices in China, India and Russia can be found e.g. in "Legal study on Government access to data in third countries" commissioned by the EDPB, and in the "EDPB Statement 02/2022 on personal data transfers to the Russian Federation". More information can also be found in reports of different international organisations, e.g. comments by the Special Procedures of the Human Rights Council, such as CHN 7/2015, CHN 18/2019, IND 31/2018, IND 3/2019, IND 7/2020, IND 8/2021, available at https://www.ohchr.org/en/special-procedures/sr-freedom-of-opinion-and-expression/comments-legislation-and-policy.

688 Information on the legislation and practices in the United Arab Emirates can be found in reports of different international organisations, e.g. comments by the Special Procedures of the Human Rights Council, such as ARE 8/2012, ARE 5/2013 and ARE 6/2020, available at https://www.ohchr.org/en/special-procedures/sr-freedom-of-opinion-and-expression/comments-legislation-and-policy and https://www.ohchr.org/en/special-procedures/sr-terrorism/comments-legislation-and-policy. More information can also be found in reports of non-governmental organisations, e.g. by the Freedom House at https://freedomhouse.org/country/united-arab-emirates/freedom-net/2022.

689 Reply by Microsoft Ireland of 26 May 2023, Annex 2, p. 8.

690 Reply by Microsoft Ireland of 26 May 2023, Annex 2, p. 9.

691 Except as regards the United States for transfers taking place prior to the entry into force of the US adequacy decision (see reply by Microsoft Ireland of 26 May 2023, Annex 2, dated from March 2023).

practices would suffer from the same lack of demonstration. The submissions made by Microsoft Ireland are therefore not such as to show that the Commission has carried out a transfer impact assessment with regard to all third countries not covered by an adequacy decision to which transfers are envisaged under the 2021 ILA, as required by the Regulation. While Microsoft Ireland as a processor could assist the Commission in carrying out a transfer impact assessment, the EDPS recalls that the ultimate responsibility of ensuring and demonstrating compliance as regards any transfers related to the Commission's use of Microsoft 365 lies with the Commission as the controller.

391. In its reply to the preliminary assessment, Microsoft Ireland argues that the EDPS should have carried out its own assessment of the level of protection in the third countries to which personal data are transferred under the 2021 ILA before imposing suspension of those transfers,[692] and that "*as such [the EDPS] fails to satisfy its burden of proof as is required under Schrems II, the Principles of Good Administration and recent CJEU case law*".[693]

392. Microsoft Ireland also argues that the EDPS should have taken into account in its assessment the changes to the "*EU benchmark*"[694] since the *Schrems II* judgment "*to determine if the degree of protection accorded in the EU legal order is in fact reduced (or at risk of being reduced) by any data transfers under the 2021 ILA*".[695]

393. In this respect, Microsoft Ireland refers to the case-law of the Court of Justice and the European Court of Human Rights and new EU laws, such as the amended Europol Regulation, adopted after the *Schrems II* judgment in relation to access by public authorities from the EU for surveillance purposes which change the level of protection in the EU benchmark.[696] Microsoft Ireland states that: "*Each of these decisions has shaped the EU Benchmark – as noted in EDPB Opinion 5/2023 on the draft EU-US Adequacy Decision (para. 139). None are discussed in the Preliminary Assessment.*"[697]

394. In relation to international developments, Microsoft Ireland refers to changes in the US legislation and the new US adequacy decision. Microsoft Ireland states that:

> "*once the Data Privacy Framework is adopted, the requirement to perform TIAs and to implement appropriate safeguards or supplementary protection measures will fall away completely*".[698]

395. In relation to international developments, Microsoft Ireland further states that:

> "*account must be taken of international developments such as the OECD Declaration on Government Access to Personal Data held by Private Sector Entities (confirmed*

---

[692] Reply by Microsoft Ireland of 26 May 2023, paras. 43, 284, 295, 305, 367, 369 and 370.
[693] Reply by Microsoft Ireland of 26 May 2023, para. 284, as well as paras. 295, 306 to 308 and 385.
[694] Reply by Microsoft Ireland of 26 May 2023, para. 279: "*The CJEU in Schrems II ruled that following a transfer outside the EU in reliance on appropriate safeguards, personal data must be granted a "level of protection essentially equivalent to that guaranteed within the European Union" and the CJEU ruled that this EU level of protection must be determined "on the basis of [the EUDPR], read in the light of the fundamental rights enshrined in the Charter" (hereinafter referred to as "EU Benchmark").*"
[695] Reply by Microsoft Ireland of 26 May 2023, paras. 35, 36, 42, as well as 372, 373, 374 and 376.
[696] Reply by Microsoft Ireland of 26 May 2023, paras. 35, 375 to 379.
[697] Reply by Microsoft Ireland of 26 May 2023, para. 379.
[698] Reply by Microsoft Ireland of 26 May 2023, paras. 381 and 382.

by the US, the EU, and Member States), which demonstrates that a large group of countries, including EU Member States, are operating under the same likeminded democratic principles of necessity and proportionality."[699]

396. The EDPS rejects these arguments.

397. In accordance with the Regulation, as clarified by the *Schrems II* judgment, the EU institution or body as the controller is the one that is primarily responsible for ensuring compliance with the Regulation as regards processing, including transfers, and an essentially equivalent level of protection of personal data transferred by the EU institution or body and others on its behalf.[700] Where the required level of protection cannot be guaranteed, it must suspend or end the transfer of personal data to the third country concerned.[701] The importance of the accountability of the controller therefore cannot be disregarded. Supervisory authorities, no matter the investigative tools at their disposal, cannot replace the accountability of the controller, which the legislator introduced precisely to make sure that the controller does not only need to comply, but must be able to demonstrate compliance.[702] That principle was enshrined in Articles 4(2) and 26(1) of the Regulation as a powerful procedural device to ensure that data protection law was actually complied with. The complexity of this investigation and the difficulty of this authority in obtaining relevant information are a witness of the importance of compliance with the accountability principle.

398. In particular, as clarified by the *Schrems* II judgment, Article 46 of the Regulation requires essential equivalence of protection to be ensured with regard to each transfer,[703] regardless of which provision in Chapter V is used to underpin transfers, to ensure that the level of protection of natural persons guaranteed by the Regulation is not undermined.[704] It follows that, regardless of which transfer tool under Article 48 of the Regulation is relied upon, a level of protection essentially equivalent to that which is guaranteed within the EEA is required.[705] The level of protection must be assessed on this basis of the provisions of the Regulation, read in light of the Charter.[706]

399. This is what constitutes the "*EU Benchmark*" on the protection for transfers of personal data outside the EEA.

400. Consequently, EDPB Recommendations 1/2020 are addressed mainly to the controllers and processors carrying out the transfers. This is because they are the ones bound by obligations under the Regulation and must assess the level of protection in the third country of destination and ensure an essentially equivalent level of protection, where necessary by implementing supplementary measures.[707] Information on such "*EU*

[699] Reply by Microsoft Ireland of 26 May 2023, paras. 381 and 382.
[700] See Articles 4(2) and 26 of the Regulation and *Schrems II* judgment, paras. 134 and 135.
[701] See Articles 4(2) and 26 of the Regulation and *Schrems II* judgment, paras. 134 and 135.
[702] Including that the implemented technical and organisational measures are effective. See Articles 4(2) and 26(1), as well as recital 45 of the Regulation.
[703] *Schrems II* judgment, paras. 94 to 96.
[704] *Schrems II* judgment, paras. 92.
[705] *Schrems II* judgment, paras. 92 to 96.
[706] *Schrems II* judgment, paras. 101 and 105.
[707] *Schrems II* judgment, para. 131 to 134.

Benchmark" concerning access by third-country authorities for surveillance purposes can be found in EDPB Recommendations 02/2020.[708]

401. It follows that the 'benchmark' is abundantly clear and it is not necessary for the EDPS to update it to the latest "*EU Benchmark*" in view of all subsequent data protection case-law. The case-law cited by Microsoft Ireland does not directly concern the question of the essential equivalence of the protection to be afforded and therefore does not undermine the EDPS' analysis of facts and of the required standards under the Regulation as interpreted, by analogy, in the *Schrems II* judgment, and the findings made in this decision.

402. As regards the case-law of the European Court of Human Rights on which Microsoft Ireland relies, as long as the EU has not acceded to the European Convention of Human Rights, the Convention does not constitute a legal instrument formally incorporated into EU law and the interpretation of EU law must be carried out in light of the fundamental rights guaranteed by the Charter.[709] Therefore, the case-law of the European Court of Human Rights cannot be relied on in determining whether the level of protection essentially equivalent to that guaranteed within the EEA.

403. As the EDPS has established, the Commission has failed to:

- sufficiently specify types of personal data and purposes of the processing in the Commission's use of Microsoft 365 (section 3.1.2.1);
- have a complete understanding of which types of personal data are transferred to which recipients in which third countries for which purposes (paragraphs 360 to 362 and 368);
- assess the level of protection in all third countries not covered by an adequacy decision to which personal data are envisaged to be transferred under the 2021 ILA and whose public authorities may make disclosure requests, and in particular whether the appropriate safeguards envisaged by the transfer tool under Article 48 of the Regulation ensure a level of protection essentially equivalent to that in the EEA under the Regulation (including the specific purpose limitation for transfers), and whether any supplementary measures are necessary (paragraphs 376, 386 to 388, 414, 553, 555 and 556);
- assess the effectiveness of implemented and envisaged supplementary measures in ensuring an essentially equivalent level of protection as required by the Regulation and *Schrems II* judgment, by taking into account EDPB Recommendations 01/2020 and other guidance of Article 29 Working Party/EDPB for conditions for their effectiveness (paragraphs 485 and 486).

404. Without carrying out the steps referred to in paragraph 403, the Commission as the controller is not in a position to determine whether an essentially equivalent level of protection is ensured, as required by Articles 46 and 48 EUDPR.

405. Moreover, the EDPS' finding that effective supplementary measures were not implemented even though they were necessary, only pertains to the United States.[710] In the *Schrems II* judgment, the Court of Justice itself had made an assessment as to the level of protection provided in the United States, and found that either supplementary

[708] https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-022020-european-essential-guarantees_en

[709] *Schrems II* judgment, paras. 98 and 99, and the case-law cited.

[710] Until the entry into force of the US adequacy decision adopted on 10 July 2023.

measures must be put in place or the transfers must stop. Controllers, processors and supervisory authorities are bound by these findings of the Court of Justice in the *Schrems II* judgment and cannot depart from the Court's analysis unless they show a significant change compared to the situation assessed by the Court.

406. The EDPS stresses that EU institutions and bodies transferring personal data to a third country, a territory or one or more specified sectors within a third country, or an international organisation for which the Commission has issued an adequacy decision must take into account the scope of the adequacy decision. Where the scope of the adequacy decision does not cover the recipient or the nature of data envisaged by the transfer, a transfer impact assessment will still have to be carried out and, in principle, a transfer tool under Article 48 of the Regulation implemented, where necessary, with supplementary measures.

407. As regards transfers to the United States taking place after the adoption on the Commission Implementing Decision EU 2023/1795 on the adequate level of protection of personal data under the EU-US Data Privacy Framework (the 'US adequacy decision'),[711] the EDPS notes that the US adequacy decision only covers transfers from the EU[712] to organisations in the United States that are included on the 'Data Privacy Framework List'.[713] While Microsoft Corporation is on that List, an EU institution or body still has to carry out a transfer impact assessment for transfers to the United States where any recipients envisaged under the 2021 ILA are not included on the Data Privacy Framework List (or to recipients that are included on that List where transfers fall outside the scope of the US adequacy decision). The EU institution or body also has to implement a transfer tool under Article 48 of the Regulation, where necessary, with supplementary measures for those transfers not covered by the US adequacy decision. When the EU institution or body assesses the level of protection related to transfers not covered by the US adequacy decision, it may take into account the Commission's assessment in the US adequacy decision of the level of protection, including in relation to the US safeguards as regards access by US authorities and redress mechanisms available to data subjects in the EU.[714]

408. As noted above, the Commission has failed to perform a transfer impact assessment as required by Articles 46 and 48 of the Regulation, including the pre-conditions necessary for its performance (see paragraph 403 of this decision). Consequently, the Commission could not ensure compliance with the Regulation, and in particular an essentially equivalent level of protection (see paragraph 404 of this decision). The EDPS has reached these findings taking into account all the circumstances of the transfers in light of the written and oral submissions by the Commission and Microsoft Ireland and the information at the EDPS' disposal as referred to in this decision.

---

[711] Commission Implementing Decision EU 2023/1795 of 10 July 2023 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework (OJ L 231, 20.9.2023, p. 118).

[712] This means that the Adequacy Decision does not cover transfers from entities located outside the EU and subject to the GDPR by virtue of Article 3(2) GDPR to organisations in the US that are included in the 'Data Privacy Framework List'. See EDPB Information note on data transfers under the GDPR to the United States after the adoption of the adequacy decision on 10 July 2023, footnote 5.

[713] https://www.dataprivacyframework.gov/s/participant-search.

[714] See, in this respect answers to questions 2 to 4 in the EDPB Information note on data transfers under the GDPR to the United States after the adoption of the adequacy decision on 10 July 2023.

409. In addition, based on various authoritative and relevant publicly available sources of information[715], the EDPS has made several references to 'problematic' laws and practices of several third countries to which transfers take place or are envisaged under the 2021 ILA, including references to specific provisions of those laws and practices. On that basis, the EDPS has drawn conclusions that they are unlikely to allow the appropriate safeguards envisaged by a transfer tool under Article 48 of the Regulation to ensure an essentially equivalent level of protection, and that supplementary measures are necessary.

410. The EDPS considers, however, that these additional considerations already go beyond the burden of proof that must be satisfied by the EDPS and the supervisory authorities under the GDPR. In particular, it follows from Articles 26 and 46 of the Regulation that it is for the controller to ensure that any transfers take place only if the Regulation, and in particular Chapter V, is complied with. The controller must not start or continue any transfers where it is not able to demonstrate that an essentially equivalent level of protection is ensured.

411. Under the 2021 ILA, transfers are envisaged to 12 countries that are not covered by an adequacy decision.[716] The EDPS considers that it is not reasonable or required by the Regulation that the EDPS[717] could only stop the transfers, in case of infringement as found in paragraph 509, after having carried out, instead of the controller, a transfer impact assessment in relation to all third countries to which transfers are contractually envisaged. Already an assessment of laws and practices of 12 third countries would constitute a significant administrative burden for a supervisory authority, and if it were required for such a number of countries, this begs the question whether the same requirement would apply where a controller would contractually allow transfers to 100 countries not covered by an adequacy decision. In this regard, the EDPS stresses that a controller is obliged to carry out such assessment only in so far as it chooses to transfer, itself or by using a processor, personal to the third countries concerned.

412. Moreover, in view of the insufficient specification by the Commission as to which types of personal data are transferred to which recipients, in which third countries and for which purposes in the Commission's use of Microsoft 365, the EDPS would in any event not be in the position to carry out a complete transfer impact assessment as required by the Regulation.

413. As regards arguments put forward by Microsoft Ireland in its reply pertaining to the suspension of data flows, the EDPS refers to paragraphs 592.1 and 595 to 598 of this decision.

Finding

[715] The EDPS relied on relevant, objective, reliable, verifiable and publicly available sources of information, such as legislation in third countries, reports of different international organisations, e.g. comments on legislation and practices of third countries by the Special Procedures of the Human Rights Council (UN Office of the High Commissioner for Human Rights), legal studies on government access to data in third countries commissioned by the EDPB, legal studies and expert opinions commissioned by Member States' DPAs, reports by public bodies in the EU and EEA, reports by non-governmental organisations and reports by professional associations.

[716] 2021 ILA, pp. 89 to 177. I.e. Australia, Brazil, Chile, China, Egypt, Hong Kong, India, Malaysia, Serbia, Singapore, South Africa, the United Arab Emirates and, prior to the entry into force of the adequacy decision adopted on 10 July 2023, the United States.

[717] As well as supervisory authorities under the GDPR.

414. It follows that on the reference date the Commission had not carried out a transfer impact assessment for transfers of personal data outside the EEA in the Commission's use of Microsoft 365. The Commission's transfer impact assessment carried out after the reference date did not assess the level of protection in all third countries not covered by an adequacy decision to which transfers of personal data are envisaged under the 2021 ILA in the Commission's use of Microsoft 365. Nor did it properly assess the level of protection in the United States as regards transfers prior to the entry into force of the US adequacy decision. The Commission has therefore failed to ensure an essentially equivalent level of protection as required by Articles 46 and 48 of the Regulation read in the light of the accountability principle in Article 4(2).

Examination of supplementary measures implemented or envisaged by the Commission

415. In accordance with Articles 26, 29, 33, 36 and 46 of the Regulation, the EU institution or body as the controller must implement and ensure that its processors implement appropriate and effective technical and organisational measures, including for security of processing and confidentiality of electronic communications, so that the processing is performed in accordance with the Regulation.[718] This includes transfers that are carried out by the controller or others on its behalf.

416. As noted in paragraph 272, where personal data are transferred to a third country not covered by an adequacy decision, supplementary measures may be necessary to ensure an essentially equivalent level of protection depending on the legislation or practices of the recipient jurisdiction.[719]

417. In its Recommendations 01/2020, the EDPB has identified five use case scenarios, describing specific circumstances and measures which the EDPB considers as effective supplementary measures where public authorities in third countries may endeavour to access transferred personal data while in transit or while in custody by the intended recipient of the data.[720] The EDPB has also identified two use case scenarios where the EDPB could not identify any effective supplementary measure to ensure an essentially equivalent level of protection.[721]

418. The EDPS in particular focuses its assessment of the supplementary measures implemented or envisaged by the Commission and Microsoft in light of the following use cases identified by the EDPB:

- Use case 1 - data storage for backup and other purposes that do not require access to data in the clear;
- Use case 2 - transfer of pseudonymised data;
- Use case 3 - encryption of data to protect them from access by the public authorities of the third country of the importer when the data transit between the exporter and their importer;
- Use case 6 - transfer to cloud services providers or other processors which require access to data in the clear; and

[718] See, in this respect, also recital 45 of the Regulation.
[719] See paras. 131 to 133 of the *Schrems II* judgment.
[720] Annex 2 to EDPB Recommendations 01/2020, use cases 1 to 5 with effective supplementary measures. See also para. 276 of this decision.
[721] Annex 2 to EDPB Recommendations 01/2020, use cases 6 and 7 with no effective supplementary measure. See also para. 279 of this decision.

- Use case 7 - transfer of personal data for business purposes including by way of remote access (and this data is not or cannot be effectively pseudonymised or effectively encrypted because the processing requires accessing data in the clear).

419. As noted in paragraph 278, if all of the cumulative conditions set out in a use case scenario, for which the EDPB found effective supplementary measures (i.e. use cases 1 to 5), are not met, the measures in question cannot be considered effective. Moreover, if the situation of the processing is different from the one covered by one of those five use case scenarios, the measures envisaged in the respective five use case scenarios might not be effective and other measures may need to be applied in order to effectively ensure an essentially equivalent level of protection.

420. The Court of Justice considered in the *Schrems II* judgment that contractual measures cannot be effective, in particular, where problematic legislation in a third country concerning access by public authorities to transferred personal data imposes on the recipient of those data obligations which are contrary to the contractual guarantees in the signed contractual clauses for transfers.[722]

421. Safeguards and measures of a contractual nature cannot effectively counter deficiencies in the level of protection stemming from problematic legislation or practices in a third country, in particular in relation to access by public authorities of that third country as such legislation may override such contractual measures.[723] Contractual safeguards and measures should therefore be accompanied by effective technical measures that prevent access to personal data within and outside the EEA by the public authorities of a third country whose legislation or practices *"are capable of impinging on the contractual guarantee of an adequate level of protection against access by the public authorities of that third country to that data"*.[724]

422. For similar reasons, organisational measures by themselves cannot effectively counter deficiencies in the level of protection for transferred data where there is problematic legislation or practices in the third country.[725] Organisational measures should therefore also be accompanied by effective technical measures.

423. Only by having implemented effective technical measures, where such measures are required, can the Commission guarantee an essentially equivalent level of protection for data outside the EEA, thus ensuring compliance with Articles 26, 29, 46 and 48 of the Regulation.

424. In its reply to the preliminary assessment, Microsoft Ireland states that:

> "*despite mentioning concerns about direct government access (Preliminary Assessment para. 226) and indirect government access (para. 214), the EDPS does not distinguish between the two, and does not mention the recently introduced differentiation in the EU Benchmark between direct access and indirect access[…], nor does it discern EU standards by scenarios.[…]*"[726]

The EDPS rejects this argument by referring to paragraphs 265, 276, 277 and 279 and to paragraphs 391 to 401. The EDPS notes that the assessment in this section of

[722] *Schrems II* judgment, para. 132 and 133. See also para. 135.
[723] *Schrems II* judgment, para. 132 and 133. See also para. 135.
[724] See, in this respect, para. 533 of this decision.
[725] See, in this respect, para. 534 of this decision.
[726] Reply by Microsoft Ireland of 26 May 2023, para. 377.

supplementary measures implemented by the Commission takes into account the criteria set out by the EDPB in its Recommendations 01/2020 for the identified technical measures to constitute effective supplementary measures. Since such criteria apply to both direct and indirect government access, there is no need to distinguish between the two types of access. Moreover, as noted in paragraph 401, the case-law cited by Microsoft Ireland to allege a differentiation in the "*EU benchmark*"[727] does not directly concern the question of the essential equivalence of the protection to be afforded. It is therefore not necessary to refer to such case-law, also in so far as it pertains to direct and indirect governmental access to personal data.

425. In its reply to the preliminary assessment, Microsoft Ireland states that: "*as confirmed by the EDPB, Microsoft as exporter is best placed to determine the measures that are adequate to protect the data it transfers to satisfy EUDPR and Schrems II requirements*".[728] The EDPS rejects this argument by referring to paragraphs 236 and 415 of this decision, and stresses that the controller is in any event ultimately responsible under Articles 4 and 26 for the processing and its compliance with the Regulation, including taking effective supplementary measures where they are required.

426. The 2021 DPIA, despite having been completed after the adoption of the final version of EDPB Recommendations 1/2020,[729] does not assess the effectiveness of supplementary measures implemented or envisaged by the Commission as required by Articles 46 and 48 of the Regulation against the criteria contained in those Recommendations.

427. As explained in paragraph 386, the Commission did not assess whether Microsoft was under a legal obligation to hand over the encryption keys which would allow the US authorities to decrypt the data themselves. Instead, the Commission stated in its 2021 DPIA that: "*Microsoft is not under any specific legal obligation to decrypt any information prior to its disclosure to the US authorities.*"[730] Had the Commission made a complete assessment of relevant US law, it would have found that it in fact does impose a legal obligation requiring entities under US jurisdiction to hand over encryption keys which allow US authorities to decrypt data.[731] The Commission wrongly concluded on the basis of this incomplete assessment that Microsoft's encryption solutions protected personal data from disclosure requests made under US law.[732] The Commission never reached the stage of analysing whether such disclosure requests were affecting or not an essentially equivalent level of protection. This led it to draw the overall conclusion that transfers to the United States under the 2021 ILA were subject to appropriate safeguards.

428. In addition to the contractual guarantees laid down in the 2021 ILA, the supplementary measures identified and implemented by the Commission are the encryption solutions

---

[727] Reply by Microsoft Ireland of 26 May 2023, paras. 35, 375 to 379.

[728] Reply by Microsoft Ireland of 26 May 2023, para. 289.

[729] The final version of EDPB Recommendations 1/2020 was adopted on 18 June 2021. The EDPS also notes that the version for public consultation was adopted on 10 November 2020 and became applicable immediately following its publication.

[730] Commission's 2021 DPIA, p. 96.

[731] In addition to the Court's assessment in the *Schrems II* judgment, see Ian Brown and Douwe Korff, Exchanges of Personal Data After the Schrems II Judgment, July 2021; Stephen Vladeck, Expert Opinion on the Current State of U.S. Surveillance Law and Authorities, commissioned by the Conference of German DPAs; the Rapport sur l'US CLOUD Act from the Federal department of justice and police of the Swiss Confederation; the Memorandum on the Application of the CLOUD Act to EU Entities commissioned by the Dutch Ministry of Justice and Security (NCSC); or the sources listed in EDPB Recommendations 01/2020 at footnote 60, p. 21.

[732] Commission's 2021 DPIA, p. 96.

offered by Microsoft, protection of sensitive non-classified documents through the Commission's implementation of Double Key Encryption ('DKE') solution and Microsoft's "Customer Lockbox" access control solution.[733] Other measures that apply to transfers have been implemented by Microsoft, in particular: the general technical and organisational measures set out in the DPA and Microsoft's compliance documentation, pseudonymisation and aggregation, technical and organisational security measures listed in Annex II to processor to processor SCCs of 13 September 2021 (including encryption), as well as unilateral and bilateral contractual protection measures (such as commitments in the processor to processor SCCs of 13 September 2021, Defending Your Data initiative, Additional Safeguards Addendum, EU Privacy Shield Certification, EU Data Boundary, Microsoft's Online Terms, White Papers and Other Commitments).[734]

429. The Commission and Microsoft Ireland consider that the supplementary and other measures they implemented to address the "*rare*", "*limited*" or "*exceptional*" international transfers of personal data which they consider are taking place under the 2021 ILA[735] effectively ensure an essentially equivalent level of protection for transferred personal data.[736] The EDPS considers that transfers under the 2021 ILA in the Commission's use of Microsoft 365, such as the transfer of logs contained in the service generated data,[737] are not rare, limited or exceptional, but that significant, large-scale transfers under the 2021 ILA are envisaged and occur on an on-going basis.[738] The EDPS finds that the measures implemented by the Commission and Microsoft are not effective for reasons explained below.

Access controls ('Customer Lockbox')

430. The 2021 DPIA states that when data must be transferred for the purposes of support cases, "*mitigation is achieved by activating the 'Customer Lockbox' feature. This feature*

[733] Commission's 2021 DPIA, sections 5.4.4.1 and 5.4.4.2, pp. 96 to 99. See also Commission's reply of 25 May 2023, section 2.3.2.

[734] See, to that effect, Commission's reply of 25 May 2023, section 2.3.2, and reply of Microsoft Ireland of 26 May 2023, sections III and VI.64, Annexes 14 to 23.

[735] See Commission's reply of 25 May 2023, paras. 100, 121, 125, 126, 143, 146 to 148, and reply of Microsoft Ireland of 26 May 2023, paras. 19, 24, 39, 72, 73, 246, 304.

[736] See Commission's reply of 25 May 2023, paras. 97 and 148, and reply of Microsoft Ireland of 26 May 2023, paras. 21, 50, 290 and 296.

[737] See, in this respect, e.g. para. 77 of this decision. The EDPS finds that that logs contained in the service generated data continuously and automatically record a large number of user activity events. The EDPS therefore considers that such logging may enable tracking the activity of data subjects that are using Microsoft 365 in extreme detail. See also Commission's reply of 25 May 2023, Annex 2. This document shows hundreds of events of user activities that result in logs containing personal data, such as accessing, copying, deleting, modifying, previewing, uploading, downloading, renaming or moving a file, moving, accessing, deleting, sending or updating an email message, creating, modifying or updating inbox rules, starting and ending calls, including listing distinct identities involved in a call or associated with an online meeting etc.

[738] See, in this respect, e.g. paras. 77, 500 and 507 of this decision. The EDPS for example finds that the Product Terms site lists several scenarios where specific services transfer certain customer data or pseudonymised personal data, either "on an ongoing basis" or temporarily, and scenarios where optional service capabilities transfer such personal data. In addition, certain services are excluded either permanently or temporarily from the EU Data Boundary. Scenarios include transfers of certain Microsoft 365 applications, Microsoft Teams, Exchange Online, SharePoint, Viva Engage, Windows Update and security services, such as Microsoft Defender.

enforces (prior) customer approval for giving time-bound access to any 'Customer data' by MS engineers".[739]

431. The 'Customer Lockbox' solution therefore allows the Commission to approve individual requests for access to "*Customer Data*" directly.[740] It applies in respect of the few occasions on which it is necessary for a support engineer to access more data than Microsoft already collects (and transfers) through extensive telemetry and debugging tools.[741] It is not supported for all Microsoft products.[742] Moreover, according to Microsoft, there are exclusion situations, in which "*Customer Lockbox requests are not triggered*".[743] By way of example, Microsoft does not make a Customer Lockbox request in "*emergency scenarios that fall outside of standard operating procedures*" and where there are "*external legal demands for data*".[744] The 2021 DPIA does not assess these exclusion situations.

432. The EDPS considers that the Commission's use of the Customer Lockbox solution is positive. However, it is not a supplementary measure as such, i.e. it does not ensure that transfers taking place are protected. Rather, it is a means of limiting the transfers that take place. It must be noted that even limited access by sub-processors constitutes access. Any type, level or duration of access is open to exploitation by state actors in the jurisdictions to which those sub-processors are subject. The 'Customer Lockbox' solution is not designed to prevent access due to orders or requests from third-country public authorities. Nor could it be, given that US law allows the data importer to be prohibited from informing the controller about disclosure requests for foreign intelligence purposes, which was relevant until the entry into force of the US adequacy decision.[745] Third-country laws, such as Australian,[746] Indian[747] and Malaysian[748] laws,

---

[739] Commission's 2021 DPIA, p. 98. See T9.

[740] More specifically for Office 365, according to Microsoft, Customer Lockbox is currently supported in Exchange Online, SharePoint Online, OneDrive for Business, and Teams, and is used to approve requests for access to customer content. See https://learn.microsoft.com/en-us/microsoft-365/compliance/customer-lockbox-requests?view=o365-worldwide#frequently-asked-questions.

[741] https://docs.microsoft.com/en-us/microsoft-365/compliance/customer-lockbox-requests?view=o365-worldwide.

[742] https://docs.microsoft.com/en-us/microsoft-365/compliance/customer-lockbox-requests?view=o365-worldwide.

[743] https://learn.microsoft.com/en-us/azure/security/fundamentals/customer-lockbox-overview.

[744] https://learn.microsoft.com/en-us/azure/security/fundamentals/customer-lockbox-overview.

[745] Section 702 FISA (50 U.S.C. ch. 36 § 1881a(i)(1)(A)) provides that:
"*With respect to an acquisition authorized under subsection (a), the Attorney General and the Director of National Intelligence may direct, in writing, an electronic communication service provider to:*
(A) immediately provide the Government with all information, facilities, or assistance necessary to accomplish the acquisition in a manner that will protect the secrecy of the acquisition and produce a minimum of interference with the services that such electronic communication service provider is providing to the target of the acquisition; and
(B) maintain under security procedures approved by the Attorney General and the Director of National Intelligence any records concerning the acquisition or the aid furnished that such electronic communication service provider wishes to maintain."
See also the responses to questions IV.1, 3 and 4 of the Expert Opinion on the Current State of U.S. Surveillance Law and Authorities commissioned by the Conference of German DPAs, pp. 18-20; Jockum Hildén, "Mitigating the risk of US surveillance for public sector services in the cloud", p. 5; and the Swiss Department of Justice's Rapport sur l'US CLOUD Act, pp. 25 and 40.

[746] See e.g. comments made by the Special Procedures of the Human Rights Council in AUS 6/2018, available at https://www.ohchr.org/en/special-procedures/sr-privacy/comments-legislation-and-policy.

[747] See e.g. pp. 32-34 of "Legal study on Government access to data in third countries" commissioned by the EDPB.

[748] See e.g. comments made by the Special Procedures of the Human Rights Council in MYS 5/2021, available

similarly prohibit a data importer from informing the controller about disclosure requests.

433. As a result, the 'Customer Lockbox' solution does not provide a means of fully complying with Articles 46 and 48 of the Regulation as interpreted by analogy in the *Schrems II* judgment and as further interpreted by EDPB Recommendations 01/2020.

434. Neither do other access control and monitoring measures provide such a means, including access logging, role-based access controls, 'Just-In-Time' access or secure admin workstations.[749] Where the data importer is obliged to provide access or to disclose data to third-country public authorities, is prohibited from informing the controller about such requests and consequently must not distinguish between access resulting from such requests[750] and access that results from regular business operations, such measures cannot provide a means of complying with the *Schrems II* judgment as interpreted by EDPB Recommendations 01/2020.

Encryption

435. The EDPS considers it positive where EU institutions and bodies use encryption solutions to ensure security and confidentiality of personal data within and outside of the EEA in accordance with Articles 4(1)(f), 33 and 36 of the Regulation. Where these encryption solutions are provided by service providers, EU institutions and bodies should carefully assess the situation in the third country to which personal data are (or are envisaged to be) transferred or from which it is (or is envisaged to be) accessed under the contract.

436. The Commission has stated in its 2021 DPIA that: "*Microsoft is not under any specific legal obligation to decrypt any information prior to its disclosure to the US authorities.*"[751] The EDPS considers this statement as misleading. Before the US data importers, which fell under the provisions of FISA 702, could benefit from the US adequacy decision of 10 July 2023, they may have been compelled to grant access to or turn over imported personal data that are in their possession, custody or control. This obligation may have extended to any cryptographic keys necessary to render the data intelligible.[752]

at https://www.ohchr.org/en/special-procedures/sr-freedom-of-opinion-and-expression/comments-legislation-and-policy.

[749] See para. 502 of this decision.

[750] EDPB Recommendations 01/2020, para. 112.

[751] Commission's 2021 DPIA, p. 96.

[752] EDPB Recommendations 01/2020, boxed text below para. 81, p. 29.

437. Other third-country laws, e.g. Australian,[753] Chinese,[754] Indian[755] and Malaysian[756] laws, similarly provide for obligations on data importers to provide access to or to turn over data upon request, including cryptographic keys.

438. Even in cases where a cloud service provider is not under a specific legal obligation to decrypt personal data prior to disclosing it to United States[757] or other third-country authorities, this fact alone does not exclude the risk of it voluntarily doing so if it has access to the cryptographic key.[758] However, such voluntary cooperation by the cloud service provider would be a clear breach of the contract with the controller.

439. It is for the EU institution or body as the controller to assess the legislation and practices in third countries. However, the Commission has not made this assessment in its 2021 DPIA, properly not even in relation to the United States for transfers taking place prior to the entry into force of the US adequacy decision,[759] even though it should have, in particular in view of the risk of unauthorised disclosure.

440. In its Recommendations 01/2020, the EDPB has identified two scenarios, describing specific circumstances and measures taken, in which the EDPB considers that the performed encryption provides an effective supplementary measure.

441. For use case 1, "Data storage for backup and other purposes that do not require access to data in the clear,"[760] the EDPB has set the following cumulative conditions for encryption to be considered an effective supplementary measure:

---

[753] See e.g. comments made by the Special Procedures of the Human Rights Council in AUS 5/2018 and AUS 6/2018, available at https://www.ohchr.org/en/special-procedures/sr-freedom-of-opinion-and-expression/comments-legislation-and-policy and https://www.ohchr.org/en/special-procedures/sr-privacy/comments-legislation-and-policy.

[754] See e.g. Laskai L. and Segal A., 2021, 'The Encryption Debate in China: 2021 Update', https://carnegieendowment.org/2021/03/31/encryption-debate-in-china-2021-update-pub-84218, referred to in footnote 109 on p. 19 of "Legal study on Government access to data in third countries" commissioned by the EDPB. See also comments made by the Special Procedures of the Human Rights Council in CHN 7/2015, CHN 18/2019, available at https://www.ohchr.org/en/special-procedures/sr-freedom-of-opinion-and-expression/comments-legislation-and-policy.

[755] See e.g. the Information Technology Act 2000 and the Information Technology (Procedures and Safeguards for Interception, Monitoring, and Decryption of Information) Rules 2009, referred to on pp. 32-34 of "Legal study on Government access to data in third countries" commissioned by the EDPB. See also e.g. https://carnegieindia.org/2021/09/13/understanding-encryption-debate-in-india-pub-85261, as well as comments made by the Special Procedures of the Human Rights Council in IND 31/2018, IND 3/2019, IND 7/2020, IND 8/2021, available at https://www.ohchr.org/en/special-procedures/sr-freedom-of-opinion-and-expression/comments-legislation-and-policy. See also comments made by the Software Freedom Law Center, India on the Draft Digital Personal Data Protection Bill 2022 and on the Draft Telecom Bill proposed by the Indian Government in November 2022

[756] See e.g. comments made by the Special Procedures of the Human Rights Council in MYS 2/2018, MYS 5/2021, available at https://www.ohchr.org/en/special-procedures/sr-freedom-of-opinion-and-expression/comments-legislation-and-policy.

[757] **With regard to the situation prior to the entry into force of the US adequacy decision.**

[758] E.g. Swiss Department of Justice's Rapport sur l'US CLOUD Act, pp. 45 and 46 or comments made by the Special Procedures of the Human Rights Council in AUS 5/2018 and AUS 6/2018, available at https://www.ohchr.org/en/special-procedures/sr-freedom-of-opinion-and-expression/comments-legislation-and-policy and https://www.ohchr.org/en/special-procedures/sr-privacy/comments-legislation-and-policy.

[759] See paras. 386 and 387 of this decision.

[760] For use case 1, the EDPB gives the example of a data exporter using a hosting service provider in a third country to store personal data, e.g. for backup purposes.

"*1. the personal data is processed using strong encryption before transmission, and the identity of the importer is verified,*

2. the encryption algorithm and its parameterization (e.g., key length, operating mode, if applicable) conform to the state-of-the-art and can be considered robust against cryptanalysis performed by the public authorities in the recipient country taking into account the resources and technical capabilities (e.g., computing power for brute-force attacks) available to them,

3. the strength of the encryption and key length takes into account the specific time period during which the confidentiality of the encrypted personal data must be preserved,

4. the encryption algorithm is implemented correctly and by properly maintained software without known vulnerabilities the conformity of which to the specification of the algorithm chosen has been verified, e.g., by certification,

5. the keys are reliably managed (generated, administered, stored, if relevant, linked to the identity of an intended recipient, and revoked), and

6. the keys are retained solely under the control of the data exporter, or by an entity trusted by the exporter in the EEA or under a jurisdiction offering an essentially equivalent level of protection to that guaranteed within the EEA."[761]

442. For use case 3 "Encryption of data to protect it from access by the public authorities of the third country of the importer when it transits between the exporter and its importer,"[762] the EDPB has set the following cumulative conditions for transport encryption, if needed with end-to-end content encryption, to be considered an effective supplementary measure:

"*1. a data exporter transfers personal data to a data importer in a jurisdiction where the law and/or practice allow the public authorities to access data while they are being transported via the internet to this third country without the European essential guarantees concerning these access, transport encryption is used for which it is ensured that the encryption protocols employed are state-of-the-art and provide effective protection against active and passive attacks with resources known to be available to the public authorities of this third country,*

2. the parties involved in the communication agree on a trustworthy public-key certification authority or infrastructure,

3. specific protective and state-of-the-art measures are used against active and passive attacks on the sending and receiving systems providing transport encryption, including tests for software vulnerabilities and possible backdoors,

4. in case the transport encryption does not provide appropriate security by itself due to experience with vulnerabilities of the infrastructure or the software used, personal

[761] For use case 3, the EDPB gives the example of a data exporter wishing to transfer data to a destination where the law and/or practices allow for access by public authorities to data while it is transiting between the country of the exporter and the country of destination.

[762] See EDPB Recommendations 01/2020, para. 90.

data is also encrypted end-to-end on the application layer using state-of-the-art encryption methods,

5. the encryption algorithm and its parameterization (e.g., key length, operating mode, if applicable) conform to the state-of-the-art and can be considered robust against cryptanalysis performed by the public authorities when data is transiting to this third country taking into account the resources and technical capabilities (e.g., computing power for brute-force attacks) available to them (see footnote 80 above),

6. the strength of the encryption takes into account the specific time period during which the confidentiality of the encrypted personal data must be preserved,

7. the encryption algorithm is implemented correctly and by properly maintained software without known vulnerabilities the conformity of which to the specification of the algorithm chosen has been verified, e.g., by certification,

8. the keys are reliably managed (generated, administered, stored, if relevant, linked to the identity of the intended recipient, and revoked), by the exporter or by an entity trusted by the exporter under a jurisdiction offering an essentially equivalent level of protection."[763]

443. The EDPS takes the criteria listed in paragraphs 441 and 442 into account in its assessment of the effectiveness of the measures implemented or envisaged by the Commission. 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 requires access to data in the clear after transfer, 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.[764]

444. Third-country laws, such as those in force in the United States at least up until the entry into force of the US adequacy decision, can also allow for interception of or access to personal data by that country's public authorities during the transit of data from the exporter to the importer's country (with or without the assistance of cloud services providers or other importers).[765] In circumstances where such laws impinge on the level of protection afforded to data subjects, it is necessary to implement robust and state-of-the-art[766] transport encryption effectively, if needed in combination with end-to-end content encryption.

Encryption solutions offered by Microsoft

445. The DPA explains that Microsoft encrypts "*Customer Data*" in transit using systems such as Transport Layer Security ('TLS'), Perfect Forward Secrecy and Internet Protocol

[763] See EDPB Recommendations 01/2020, para. 90.
[764] See EDPB Recommendations 01/2020, paras. 81, 84, 94 and 95.
[765] See EDPB Recommendations 01/2020, para. 90, pp. 32 and 33, and footnote 55, p. 18.
[766] For guidance on robust and state-of-the-art technical and organisational measures, in particular cryptographic mechanisms, see technical guidance published by official cybersecurity authorities of the EU and its Member States, e.g. ENISA Guideline on "State of the art" in IT security (2021) or guidance given by the German Federal Office for Information Security in its Technical Guidelines of the TR-02102 series.

Security.[767] It also explains that Microsoft "*encrypts Customer Data stored at rest in Online Services*".[768]

446. The 2021 DPIA refers to the use of TLS with a minimum 2048-bit length of cryptographic keys in certificates generated by Microsoft.[769] It cites this as a mitigating measure to reduce the risk of a third party accessing data in transit or using the keys.[770]

447. The 2021 DPIA shows that the Commission has considered which type of TLS encryption will apply to various Microsoft products it uses. The 2021 DPIA mentions that: "*Microsoft moves to TLS 1.2 for connectivity to M365*".[771] It states that: "*Microsoft will no longer support TLS 1.0/1.1 in Microsoft Teams Desktop application starting July 1, 2021*".[772] It refers to the need for the Commission's services to "*upgrade all clients using TLS 1.0/1.1 and 3DES to connect to Office 365 to use better protocols(TLS 1.2 or higher) and cipher*".[773] It also refers to the Microsoft website, which provides further information in relation to use of TLS in Microsoft 365.[774]

448. However, the 2021 DPIA does not assess risks related to Microsoft being the certificate authority for use of TLS implemented in Microsoft 365 products and thus acting as the trusted third party that stores, signs, and issues digital certificates.[775] Nor does the 2021 DPIA assess the risks of Microsoft (as one of the parties involved in the communication in the Commission's use of Microsoft 365 products or otherwise as provider of these products) being able to access the certificates or keys and decrypt the data. The 2021 DPIA also does not assess whether the transport encryption[776] as made available by

---

[767] See section on "*Data Encryption*" in the main body of the DPA, 2021 ILA, p. 32.
[768] See section on "*Data Encryption*" in the main body of the DPA, 2021 ILA, p. 32.
[769] See 2021 DPIA, pp. 32, 96 and 97.
[770] See 2021 DPIA, pp. 32, 96 and 97.
[771] See 2021 DPIA – Annexes II+III, row 50, column R of the "10. Security Risk Register".
[772] See 2021 DPIA – Annexes II+III, row 50, column R of the "10. Security Risk Register".
[773] See 2021 DPIA – Annexes II+III, row 50, column P of the "10. Security Risk Register".
[774] According to this information (as published by Microsoft on 5 July 2022 and accessed by the EDPS on 20 September 2022), Microsoft started to deprecate the use of TLS 1.0 and 1.1 as of January 2020 and the connection to Office 365 through TLS 1.0 and 1.1 from October 2020. According to Microsoft, "[a]*s of October 31, 2018, the Transport Layer Security (TLS) 1.0 and 1.1 protocols are deprecated for the Microsoft 365 service.* [...] *The effect for end-users is minimal. This change has been publicized for over two years, with the first public announcement made in December 2017.*". However, according to an update by Microsoft (published on 30 September 2020 and accessed by EDPS on 14 October 2022), "[d]*ue to COVID-19, Microsoft postponed the deprecation of TLS 1.0/1.1 for Microsoft 365/Office 365. However, as supply chains have adjusted and certain countries open back up, TLS enforcement has been reset to start October 15, 2020.*".
Microsoft recommends that all client-server and browser-server combinations use TLS 1.2 (or a later version) in order to maintain connection to Office 365 services; Microsoft will, however, continue accepting SMTP Connection which is unencrypted without any TLS, although they do not recommend email transmission without any encryption. According to this information (as updated by Microsoft on 3 October 2022 and accessed by the EDPS on 14 October 2022), Microsoft announced, "[they] *have already disabled TLS 1.0 and 1.1 for most Microsoft 365 services in the world wide environment. Rollout will continue over the following weeks and months. For Microsoft 365 operated by 21 Vianet, TLS 1.0/1.1 will be disabled on June 30, 2023.*". Furthermore, the Office client relies on the Windows web service to send and receive traffic over TLS protocols. The Office client can use TLS 1.2 if the web service of the local computer can use TLS 1.2. However, according to Microsoft (published on 25 May 2022 and accessed by the EDPS on 19 October 2022), TLS protocol version 1.3 is only supported on Windows Server 2022 and Windows 11.
[775] The digital certificates contain a public key and the identity of the owner of the certificate.
[776] TLS allows client/server applications to communicate over the Internet in a way that is designed to prevent eavesdropping, tampering, and message forgery. The Internet Engineering Task Force specified TLS protocol version 1.2 in August 2008, making earlier versions of the TLS protocol obsolete (see RFC 5246). In August 2018, the Internet Engineering Task Force specified TLS protocol version 1.3 and specified new requirements for TLS 1.2 implementations, also making the earlier versions obsolete (see RFC 8446). The

Microsoft 365 products is state-of-the-art and effective for the purposes of securing data in transit from interception. The EDPS takes note of submissions by Microsoft Ireland in its reply to the preliminary assessment that "*Customer Data will be encrypted when in transit between customer and Microsoft (using Transport Layer Security, TLS 1.2 or higher) and between Microsoft data centres (using TLS or Internet Protocol Security, IPSec)*".[777] These submissions, however, do not change the EDPS' findings of failure in the Commission's assessment of transport encryption.

449. There is no explanation in the 2021 ILA on whether encryption is implemented in respect of data other than "*Customer Data*", such as diagnostic data, service generated data or professional services data. Yet, as mentioned in paragraph 27, the Commission and Microsoft Ireland agree that data falling within the contractual definitions of these terms contain personal data. The EDPS therefore expected the Commission's transfer impact assessment to include an assessment of whether and when the data are encrypted and whether the encryption satisfies the criteria in use case 1 or 3 of EDPB Recommendations 01/2020. Statements in the 2021 DPIA as regards encryption are limited to certain types of data and are not substantiated.[778] They therefore do not constitute such an assessment.

450. The 2021 ILA explains that: "*Microsoft offers customer-managed encryption keys for certain services.*"[779] With respect to the degree of control that these keys provide, the 2021 ILA states that: "*as described in applicable service documentation, customer-managed encryption keys are intended for Customer to revoke upon exit from use of Online Services.*" The Commission has explained that:

> "*While customer-managed keys are intended to enable customers to have greater assurance/control over Customer Data, they are not intended to prevent decryption of the Customer Data by Microsoft as required for routine service fulfilment.*"[780]

Customers therefore only control the keys to the extent that they can revoke them when they cease to use Microsoft services. Microsoft retains access to data in the clear in the course of routine service provision. The EDPS understands that "*customer-managed*" encryption keys are stored in the Microsoft Azure cloud.[781]

451. The 2021 DPIA makes clear that, except in respect of sensitive non-classified documents,[782] the Commission relies on the encryption solutions offered by Microsoft.[783]

---

best current practice published by the Internet Engineering Task Force in March 2021 sets out that TLS protocol versions 1.0 and 1.1 must not be used (see RFC 8996). In particular, section 4 of RFC 8996 sets out: "*TLS 1.0* ***MUST NOT*** *be used. Negotiation of TLS 1.0 from any version of TLS* ***MUST NOT*** *be permitted.*" and section 5 sets out "*TLS 1.1* ***MUST NOT*** *be used. Negotiation of TLS 1.1 from any version of TLS* ***MUST NOT*** *be permitted.*".

777 Reply by Microsoft of 26 May 2023, Annex 5, para. 110, as well as paras. 120 and 124.

778 The 2021 DPIA, p. 96, e.g. states that service generated data transfers are protected by encryption in transit. It does not, however, mention encryption at rest, nor does it assess the effectiveness of the encryption as a supplementary measure in light of conditions set out in EDPB Recommendations 01/2020.

779 2021 ILA, p. 33.

780 Commission's 'Note to the EU Institutions, agencies and other bodies participating in the Microsoft ILA' of 6 May 2020, Annex, p. 11. Similarly, Microsoft responses under section 6 of Annex 4 to Commission's 2020 DPIA, pp. 8 and 9.

781 See in this respect e.g. https://learn.microsoft.com/en-us/microsoft-365/compliance/customer-key-overview?view=o365-worldwide.

782 Commission's 2021 DPIA, section 7.2.3, pp. 121-122.

783 Commission's 2021 DPIA, section 5.4.4.1, p. 96.

However, the Commission implemented the Double Key Encryption solution for sensitive non-classified documents only in August 2021 (see paragraph 295), i.e. after the reference date. The EDPS therefore understands that by the reference date, the Commission relied solely on encryption solutions offered by Microsoft.

452. To conclude: the circumstances of the Commission's use of encryption are as follows. The Commission uses encryption solutions offered by Microsoft. The Commission does not retain sole control of the cryptographic keys for encryption in transit or at rest. Microsoft is in possession of them and either retains access to personal data in the clear following the transfer or encrypts them with keys they have access to. The number of products and services offered by Microsoft, and its stated need to conduct transfers for the purposes of developer, support, security and support operations,[784] imply that in some cases Microsoft accesses personal data in the clear after transfer.[785] The EDPS considers that in this particular case the cumulative conditions set out in use case 1 and in use case 3 of EDPB Recommendations 01/2020 are not met.

453. According to the Commission, the United States is the principal transfer destination: problematic legislation, as characterised in the *Schrems II* judgment,[786] therefore applied to such transfers, granting power to public authorities beyond what was necessary and proportionate in a democratic society.[787]

454. Since the conditions set out in use cases 1 and 3 of EDPB Recommendations 01/2020,[788] respectively, are not all cumulatively met, the situation cannot be considered as falling under one of those use cases. The EDPS considers that these situations fall under use cases 6 and 7 of EDPB Recommendations 01/2020[789] given that Microsoft requires access to personal data in the clear to provide its services and to process the data for its own business purposes. Consequently, the EDPS does not consider the Commission's use of Microsoft's encryption solutions analysed above to constitute effective supplementary measures required to ensure an essentially equivalent level of protection.

455. In addition, German data protection authorities have reached a similar conclusion in their assessment of Microsoft 365.[790]

Commission's implementation of Double Key Encryption solution after the reference date

---

[784] Commission's additional reply of 7 June 2022, Annex 4, p. 10.

[785] See in this respect similarly the findings of the Conference of German DPAs on Microsoft Online Services (Microsoft 365), 24 November 2022, in summary (p. 7) and assessment (pp. 37, 38, 54 to 57). See similarly the findings of the Baden-Württemberg DPA's audit of Microsoft 365 in the context of a pilot project on its possible use in schools (23 April 2021, published 25 April 2022), in particular in the Baden-Württemberg DPA's opinion (p. 8).

[786] See para. 264 for explanation of how problematic legislation and practices are to be understood in line with EDPB Recommendations 01/2020.

[787] **The EDPS makes this observation with regard to the situation prior to the entry into force of the US adequacy decision.**

[788] See EDPB Recommendations 01/2020, pp. 30 and 32-33. See also paras. 440 and 444 of this decision.

[789] See EDPB Recommendations 01/2020, pp. 34-36.

[790] See the findings of the Conference of German DPAs on Microsoft Online Services (Microsoft 365), 24 November 2022, in summary (p. 7) and assessment (p. 37, 38, 54 to 57). See similarly the findings of the Baden-Württemberg DPA's audit of Microsoft 365 in the context of a pilot project on its possible use in schools (23 April 2021, published 25 April 2022), in particular in the Baden-Württemberg DPA's opinion (p. 8).

456. After the reference date, the Commission implemented Double Key Encryption (DKE) solution to protect sensitive non-classified documents (see paragraph 295). The EDPS understands that this DKE solution relies on the DKE technology provided by Microsoft that is integrated with on-premise Hardware Security Module services.[791] The 2021 DPIA states that it uses "*an encryption key that is under the exclusive control of the Commission.*"[792] In its reply to the preliminary assessment, the Commission has also stated that: "*it has also implemented robust encryption by relying on [DKE] technique to ensure overall protection of sensitive content. [...] DKE applies a second layer of encryption to sensitive non-classified documents in M365, using a key under the exclusive control of the Commission.*"[793]

457. This solution could potentially serve as an effective supplementary measure for international transfers to ensure an essentially equivalent level of protection. The Commission would need to ensure that it meets the criteria of use case 1 or 3 of EDPB Recommendations 01/2020[794] or provide an alternative but equally convincing assessment of its effectiveness. Fulfilment of the conditions indicated in the use case would involve taking organisational measures to ensure that the key was not exported to or otherwise available to Microsoft and that any vulnerabilities in the encryption algorithm and its implementation were patched continuously so that the encryption remained a state-of-the-art measure.[795] The Commission would have to take such measures also where it relies on any hardware and other infrastructure provided by Microsoft to deploy and manage double-key encryption[796] or on encryption in confidential computing solutions provided by Microsoft.[797]

458. The Commission has confirmed that DKE applies only to sensitive non-classified information, which is a small portion of the data processed by Microsoft in the context of the provision of all services to the Commission, and that this is likely to remain the case for the foreseeable future.[798]

459. The Commission's implementation of DKE solution is promising. However, given the narrow scope of its deployment, limited to sensitive non-classified information, it cannot serve as a means to bring all transfers under the 2021 ILA into compliance with the Regulation. The EDPS has also not been provided with sufficient information to take a view on its effectiveness as a supplementary measure in the cases where it is deployed.

Roll-out of end-to-end encryption for Teams calls

[791] See Commission's 2021 DPIA, section 7.2.3, p. 122; "*DIGIT's initial implementation of DKE relied on a server (in Welcome) without integration with on-premises HSM services. To achieve maximum security of the key under the Commission's exclusive control, DIGIT works on integration with Thales Luna HSM as a priority.*"

[792] Commission's 2021 DPIA, section 7.2.3, p. 122.

[793] Commission's reply of 25 May 2023, para. 74, as well as para. 143, second bullet point. At the hearing of 23 October 2023, the Commission also referred to the "*the introduction of [...] DKE, for the protection of documents holding sensitive non-classified data in accordance with our corporate governance decisions*".

[794] EDPB Recommendations 01/2020, p. 30 and 32-33.

[795] See also conditions 2 to 4 in the use case 1 and, similarly, conditions 1 to 5, 7 and 8 of use case 8 of EDPB Recommendations 01/2020.

[796] E.g. Microsoft's Hardware Security Module and Azure Key Vault services.

[797] E.g. Azure Confidential Computing services.

[798] Minutes of the evidence-gathering meeting held on 28 November 2021, p. 7.

460. The Commission's 2021 DPIA mentions Microsoft's plan to protect calls in Teams through end-to-end encryption in the future. The DPIA suggests that this could allow users to work on sensitive non-classified matters using Teams.[799]

461. This encryption solution might also serve as an effective supplementary measure to ensure an essentially equivalent level of protection if shown to fall within use case 1 or 3 of EDPB Recommendations 01/2020.[800] The EDPS takes note that the Commission has stated in its reply to the preliminary assessment that "[it] *has instructed Microsoft to implement end-to-end encryption for bilateral calls as well as for conference calls in Microsoft Teams*".[801] However, at the time of issuing this decision, the Commission has not provided the EDPS with further information about the actual start of use of this solution for all calls in the Commission's use of Teams nor about how this solution has been implemented. The EDPS has thus not been provided with sufficient information to take a view on the effectiveness of end-to-end encryption solution for Teams calls as a supplementary measure in the cases where it is deployed. The Commission should assess this solution against the criteria provided in those use cases of EDPB Recommendations 01/2020.

Pseudonymisation

462. It is possible for pseudonymisation performed prior to transfer to constitute an effective supplementary measure, provided that all the conditions for its effectiveness are fulfilled (see use case 2 of EDPB Recommendations 01/2020)[802] The EDPB has set the following cumulative conditions:

> "*1. a data exporter transfers personal data processed in such a manner that the personal data can no longer be attributed to a specific data subject, nor be used to single out the data subject in a larger group without the use of additional information,*
>
> *2. that additional information is held exclusively by the data exporter and kept separately in a Member State or in a third country, by an entity trusted by the exporter in the EEA or under a jurisdiction offering an essentially equivalent level of protection to that guaranteed within the EEA,*
>
> *3. disclosure or unauthorised use of that additional information is prevented by appropriate technical and organisational safeguards, it is ensured that the data exporter retains sole control of the algorithm or repository that enables re-identification using the additional information, and*
>
> *4. the controller has established by means of a thorough analysis of the data in question - taking into account any information that the public authorities of the recipient country may be expected to possess and use - that the pseudonymised*

[799] See Commission's 2021 DPIA, section 7.2.4, pp. 122 to 123.
[800] EDPB Recommendations 01/2020, pp. 30 and 32-33.
[801] See Commission's reply of 25 May 2023, para. 76, as well as para. 148 and footnote 76 to para. 170. At the hearing of 23 October 2023, the Commission also referred to the "*also the rollout of Teams Premium that provides end-to-end encryption for robust protection of video conferencing and meeting data*".
[802] EDPB Recommendations 01/2020, p. 31, use case 2 "Transfer of pseudonymised Data"

personal data cannot be attributed to an identified or identifiable natural person even if cross-referenced with such information."[803]

463. The Commission has stated that service generated data that are transferred to third countries are pseudonymised prior to transfer.[804] The Commission's 2021 DPIA explains that the process of pseudonymisation for service generated data is carried out by Microsoft on Microsoft servers in EU data centres.[805] The DPIA does not, however, detail the process by which Microsoft pseudonymises the data or assess its effectiveness against the conditions set by the EDPB for pseudonymisation to constitute an effective supplementary measure.[806] The EDPS has analysed information provided by Microsoft Ireland in its reply to the preliminary assessment and at the hearing[807] as regards pseudonymisation carried out by Microsoft, in paragraphs 127 to 173. The EDPS has found that that pseudoymisation is not effective as a means of rendering data anonymous, because Microsoft has means reasonably likely to be used to identify a natural person directly or indirectly.[808]

464. A pre-condition for pseudonymisation to be effective as a supplementary measure is therefore that the data importer and third-country public authorities be unlikely to have the means to re-identify data subjects, including by singling out, using the pseudonymised data. Pseudonymisation is not an effective measure when the provider carrying it out has the additional information that allows re-identification, including by singling out, of data subjects or is processing personal data concerning the same data subjects in the clear, i.e. in non-pseudonymised and unencrypted form.[809] Nor is it an effective measure if a public authority of a third country has such additional information.[810] Additional data may consist of tables juxtaposing pseudonyms with the identifying attributes they replace, cryptographic keys or other parameters for the transformation of attributes, or other data permitting the attribution of the pseudonymised data to identified or identifiable natural persons.[811]

465. The EDPS considers that in this particular case none of the cumulative conditions of conditions set out in use case 2 of EDPB Recommendations 01/2020 are met. The Commission does not have sole control of the algorithm or repository of information that would allow re-identification. Microsoft retains both the non-pseudonymised and pseudonymised personal data[812] relating to individuals, look-up tables, identity of users and other information which enable it to identify the natural persons using its services by resolving the pseudonyms.[813] Microsoft also retains the secret keys to decrypt pseudonyms in service generated data, which also enable it to identify the natural

[803] See EDPB Recommendations 01/2020, para. 85.
[804] Commission's 2021 DPIA, pp. 93-94.
[805] Commission's 2021 DPIA, p. 93.
[806] See Use Case 2 in Annex 2 to EDPB Recommendations 01/2020, pp. 31-32.
[807] See reply by Microsoft of 26 May 2023, paras. 54 to 55 and Annexes 3, 5 and 7, as well as paras. 131, 135, 138 to 148 of this decision.
[808] See paras. 154 to 173 of this decision.
[809] See EDPB Recommendations 01/2020, Use Cases 2, 6 and 7 in Annex 2.
[810] See EDPB Recommendations 01/2020, paras. 87 and 88, p. 31.
[811] See EDPB Recommendations 01/2020, paras. 85, footnote 83.
[812] See, in this respect, paras. 131, 141, 142, 148, 149 and 156 to 158, as well as 132 of this decision. The underlying raw data and intermediate pseudonymous data. This data includes end-user identifiers, such as User GUIDs, PUIDs, or SIDs, Session IDs, which when combined with other information, such as a mapping table, identify the end user. See, in this respect, also the Commission's 2021 DPIA, section 3.10.2, p. 53 (also reproduced in the reply by Microsoft Ireland of 26 May 2023, para. 165, p. 49).
[813] See, in this respect, paras. 148 and 158 of this decision.

persons using its services.[814] All of these are additional information in Microsoft's possession which Microsoft can attribute to an individual or with which an individual can be singled out.[815] The data exporter (Microsoft Ireland) and the data importer (Microsoft Corporation) are part of the same corporate group. The data importer therefore has foreseeable means by which to access the additional information held by the data exporter that would allow re-identification, including by singling out, of data subjects.[816] Before the adequacy decision benefitting the United States, the US authorities could have requested that information using US legal tools such as those available under Section 702 FISA, the Stored Communication Act or the CLOUD Act. [817] For example, Microsoft Corporation could have been compelled to order Microsoft Ireland to provide that information.[818] Authorities of other third countries, e.g. Australia,[819] China,[820] India,[821] or Malaysia[822] could similarly request that information using their own legal tools.

466. In addition, the Commission has noted that for the purposes of Microsoft's business operations, both pseudonymised and non-pseudonymised personal data are transferred to the United States.[823] Prior to the amendment to the 2021 ILA of 19 December 2023, pseudonymised personal data were processed for four out of the six business purposes; non-pseudonymised personal data were processed for the remaining two business

---

[814] See in this respect para. 158 of this decision.

[815] See in this respect recital 16 of the Regulation, as well as paras. 127 and 132 of this decision. See in this respect also Article 29 Working Party's Opinion 05/2014, p. 29, fifth para.

[816] See, in this respect, also the EDPS' findings in paras. 162 to 173 of this decision.

[817] **The EDPS makes this observation with regard to the situation prior to the entry into force of the US adequacy decision.**

[818] In a recent decision of the French Conseil d'État, it was held that the use by an EU company of a server in the EU that was managed by an EU-based subsidiary of a US parent company (in casu, Amazon Web Services Luxembourg SARL, a subsidiary of Amazon Web Services Inc. in the USA) also exposed the data on the server to access by the authorities in the US, because the parent company was subject to US surveillance laws and could be ordered to order its subsidiary to allow access. Conseil d'État order of 12 March 2021 in urgency proceedings (acting as "*juge des référés*") N° 450163, Association Interhop et autres, at: https://www.dalloz.fr/documentation/Document?id=CE_LIEUVIDE_2021-03-12_450163#texte-integral. Cited in Ian Brown and Douwe Korff, Exchanges of Personal Data After the *Schrems II* Judgement, p. 43. See also the responses to questions I.5.f and 6 in the Expert Opinion on the Current State of U.S. Surveillance Law and Authorities commissioned by the Conference of German DPAs, pp. 9-10; the Swiss Department of Justice's Rapport sur l'US CLOUD Act, pp. 6, 7 and 17; and the Memorandum on the Application of the CLOUD Act to EU Entities commissioned by the Dutch Ministry of Justice and Security (NCSC), pp. 4 and 9-11.

[819] See e.g. comments made by the Special Procedures of the Human Rights Council in AUS 5/2018, AUS 6/2018, available at https://www.ohchr.org/en/special-procedures/sr-freedom-of-opinion-and-expression/comments-legislation-and-policy and https://www.ohchr.org/en/special-procedures/sr-privacy/comments-legislation-and-policy.

[820] See e.g. comments made by the Special Procedures of the Human Rights Council in CHN 7/2015, CHN 18/2019, available at https://www.ohchr.org/en/special-procedures/sr-freedom-of-opinion-and-expression/comments-legislation-and-policy.

[821] See e.g. pp. 29-34 of "Legal study on Government access to data in third countries" commissioned by the EDPB, Traceability and Cybersecurity: Experts' Workshop Series on Encryption in India by the Internet Society, as well as comments made by the Special Procedures of the Human Rights Council in IND 31/2018, IND 3/2019, IND 8/2021, available at https://www.ohchr.org/en/special-procedures/sr-freedom-of-opinion-and-expression/comments-legislation-and-policy.

[822] See e.g. comments made by the Special Procedures of the Human Rights Council in MYS 5/2021, available at https://www.ohchr.org/en/special-procedures/sr-freedom-of-opinion-and-expression/comments-legislation-and-policy.

[823] Commission's 2021 DPIA, see table on p. 93.

purposes.[824] Following that amendment, pseudonymised data are processed for all four remaining business purposes.[825] Moreover, Microsoft processes non-pseudonymous personal data to comply with its legal obligations and to combat fraud, cybercrime and cyberattacks.[826] It is therefore foreseeable that the data that are processed in the clear could contain additional information allowing the re-identification, including by singling out, of individuals from the pseudonymised data.[827]

467. The Commission should have considered that US authorities may also already hold such additional information allowing the re-identification, including by singling out, of individuals from the pseudonymised data.[828]

468. On the basis of the available information, the EDPS considers that the circumstances fall under the scenarios described in use cases 6 and 7 of EDPB Recommendations 01/2020. The EDPS has taken into account that Microsoft requires access to personal data in the clear to provide its services and to process the data for its own business purposes, and that the conditions set out in use case 2 are not all cumulatively met.[829] The EDPS therefore does not consider the pseudonymisation performed by Microsoft to be an effective supplementary measure required to ensure an essentially equivalent level of protection in accordance with Articles 46 and 48 of the Regulation.

469. The EDPS has assessed the aggregation by Microsoft of pseudonymised data, which it considers as a protection measure for transfers, in paragraphs 127 to 173 and found that aggregation does not effectively result in anonymisation, because Microsoft has means reasonably likely to be used to identify a natural person directly or indirectly.

Direct compensation mechanism and contractual measures

470. Clauses 2 to 4 of the Additional Safeguards Addendum to the SCCs concluded between the Commission and Microsoft Corporation created a mechanism by which Microsoft would indemnify a data subject for damage caused by a disclosure of personal data that it makes in response to an order from a non-EEA governmental body or law enforcement agency.[830] Following the conclusion of the SCCs between Microsoft Ireland and Microsoft Corporation which replaced the SCCs between the Commission and Microsoft Corporation, this compensation mechanism has been incorporated with the same wording into the 2021 ILA under Clauses 1 to 3 of the new Additional Safeguards Addendum to the DPA.[831]

---

[824] Commission's 2021 DPIA, see table on p. 93.
The EDPS makes this observation with regard to the situation prior to the entry into force of the US adequacy decision.

[825] Commission's email of 19 December 2023, Annex 2 (Amendment to Contract Documents), pp. 1 and 2, point 2; see as well similar amendments for software and professional services, respectively, on pp. 4 and 5, point 7, and pp. 5 and 6, point 9. See also para. 162 of this decision.

[826] See paras. 131, 157, 158 and 164 of this decision.

[827] As the EDPB has noted, "*physical location [natural persons] or their interaction with an internet based service at specific points in time may allow the identification of that person even if their name, address or other plain identifiers are omitted. This is particularly true whenever the data concern the use of information services (time of access, sequence of features accessed, characteristics of the device used etc.).*" EDPB Recommendations 01/2020 paras. 86 and 87.

[828] See also condition 4 in the use case 2 and para. 88 of EDPB Recommendations 01/2020.

[829] For use cases 6 and 7 see pp. 34 to 36 of EDPB Recommendations 01/2020. For use case 2 see pp. 31 to 32.

[830] 2021 ILA, p. 79.

[831] Reply by Microsoft Ireland of 26 May 2023, Annex 1B, pp. 48 to 49.

471. According to this mechanism, the data must have been transferred out of the EEA under the SCCs and the disclosure must qualify as a violation of Chapter V of the Regulation. The damage can be material or not.

472. This contractual mechanism can only result in monetary compensation. It cannot substitute a data subject's right to an effective administrative and judicial redress for unlawful processing of their personal data.[832] This mechanism cannot therefore amount to an effective legal remedy within the meaning of Article 48 of the Regulation.

473. These clauses offer a limited additional protection for data subjects. They cannot in themselves remedy the failure of a third country's legal order to provide for a level of protection essentially equivalent to that guaranteed within the EEA, where that legal order does not provide for a redress mechanism against surveillance measures. Therefore, this contractual measure does not amount to an effective supplementary measure.[833] [834]

474. In its reply to the preliminary assessment, Microsoft Ireland also lists several "*contractual protection measures*".[835] The EDPS does not consider such measures to be effective supplementary measures. This is because by their inherent nature, any contractual measures cannot bind third-country public authorities.[836]

Other measures applicable to transfers

475. In their replies to the preliminary assessment, the Commission and Microsoft Ireland point out that the above supplementary measures are not the only measures applicable to transfers.

476. The Commission points out that "*Annex II of the SCCs P2P also includes a set of technical and organisational measures to ensure the security of the personal data processed, addressing specifically – among others - Information Security, Asset Management, Human Resources Security, Physical Security and Access Control*".[837]

477. The EDPS has taken note of other measures implemented by Microsoft, which Microsoft Ireland refers to in its reply to the preliminary assessment as measures that also ensure the protection of transferred data:

a) technical protection measures (privacy-by-design,[838] pseudonymisation and aggregation,[839] encryption,[840] security measures listed in Annex II to processor to processor SCCs of 13 September 2021[841]);
b) contractual protection measures that Microsoft implemented as unilateral and bilateral commitments[842] (commitments in the Microsoft intra-group transfer

[832] See paras. 187 to 189 of the *Schrems II* judgment and recital 104 of the Regulation.
[833] EDPB Recommendations 01/2020, paras. 99 and 119, pp. 36 and 41.
[834] See, in this respect, similarly the findings of the Conference of German DPAs on Microsoft Online Services (Microsoft 365), 24 November 2022, in summary (p. 7) and assessment (p. 55).
[835] Reply by Microsoft Ireland of 26 May 2023, paras. 62 to 69 and 298 to 300.
[836] See *Schrems II* judgment, para. 132.
[837] Commission's reply of 25 May 2023, para. 148, as well as para. 140.
[838] Reply by Microsoft Ireland of 26 May 2023, paras. 52 and 53, and Annexes 14, 15, 16 and 17.
[839] Reply by Microsoft Ireland of 26 May 2023, paras. 54 and 55, and Annexes 3 and 5.
[840] Reply by Microsoft Ireland of 26 May 2023, paras. 57 to 60, and Annexes 5, 15, 18 and 19.
[841] Reply by Microsoft Ireland of 26 May 2023, para. 61, and Annex 13.
[842] See para. 421 of this decision.

SCCs (i.e. processor to processor SCCs of 13 September 2021),[843] Defending Your Data initiative and Additional Safeguards Addendum as reflected into the DPA,[844] EU Privacy Shield Certification commitments,[845] EU Data Boundary,[846] Microsoft's Online Terms, White Papers and Other Commitments,[847] Microsoft Privacy Trust Center and adherence to the EU Cloud Code of Conduct for Microsoft Azure[848]), and

c) organisational protection measures[849] as reflected in the DPA and Microsoft's compliance documentation,[850] and as reflected in meeting industry standards for data security.[851]

478. The EDPS considers that measures annexed to the processor to processor SCCs of 13 September 2021, as well as measures reflected in the DPA and Microsoft's compliance documentation, to a large extent reflect the measures that the Commission identified and assessed in its 2021 DPIA. The EDPS does not consider those measures to be effective in ensuring an essentially equivalent level of protection (see paragraphs 445 to 473). Crucially, neither the measures annexed to those SCCs or reflected in the DPA and

[843] Reply by Microsoft Ireland of 26 May 2023, paras. 63 to 66 and Annex 1.B.

[844] Reply by Microsoft Ireland of 26 May 2023, paras. 67 to 69 and 298 to 300, and Annex 20.

[845] Reply by Microsoft Ireland of 26 May 2023, para. 70 and Annex 21.

[846] Reply by Microsoft Ireland of 26 May 2023, paras. 71 to 74 and 301 to 304, and Annexes 1 and 3.

[847] Reply by Microsoft Ireland of 26 May 2023, paras. 75 to 79, and Annexes 2, 3 and 4. The EDPS takes note of the Transfers White Paper, Service Generated Logs White Paper and Business Operations White Paper submitted by Microsoft. The EDPS considers that these papers are organisational measures that provide Microsoft's clarifications for controllers in relation to the processing and transfers in use of Microsoft 365 and in relation to measures and commitments Microsoft has taken in that respect. However, the white papers do not constitute measures to supplement the relied-on transfer tool to effectively ensure an essentially equivalent level of protection.

[848] Reply by Microsoft Ireland of 26 May 2023, para. 81 and Annex 22. The EDPS takes note of Microsoft's adherence to the EU Cloud Code of Conduct for Microsoft Azure. In line with Article 29(5) of the Regulation, a processor's adherence to an approved code of conduct under Article 40(5) GDPR may be used as an element by which to demonstrate sufficient guarantees as referred to in Article 29(1) and (4) of the Regulation. In the EDPS' view, however, Microsoft's adherence to the EU Cloud Code of Conduct does not cover Microsoft 365. Neither does the EU Cloud Code of Conduct provide appropriate safeguards for transfers to non-adequate countries, and therefore does not constitute a transfer tool under Article 46(2)(f) GDPR. A code of conduct (composed of safeguards and measures of a contractual and organisational nature) could also not effectively counter deficiencies in the level of protection where there is problematic legislation or practices in the third country as regards access by public authorities of that third country. See, in that respect, paras. 421 and 422 of this decision.

[849] See para. 422 of this decision.

[850] Reply by Microsoft Ireland of 26 May 2023, para. 82 and Annex 23.

[851] Reply by Microsoft Ireland of 26 May 2023, paras. 81 and 82. See also Commission's reply of 25 May 2023, paras. 138 and 139. Microsoft Ireland and the Commission in particular refer to Microsoft's certification under ISO 27001, ISO 27002, ISO 27018, SOC 1 Type II and SOC 2 Type II standards. Certifications under international or industry standards for data security are organisational measures that controllers or that (sub-)processor may take to obtain assurances that their processes and controls comply with information security requirements, including privacy. However, the EDPS notes that certifications under international or industry standards are not certifications under approved certification mechanism referred to in Article 42 of the GDPR, so their aim is not to assess and demonstrate compliance of processing operations with the GDPR or existence of appropriate safeguards for transfers of personal data outside the EEA. As such, certifications under international or industry standards for data security may provide EU institutions and bodies an element by which to assess, taking into account the scope and any reservations or limitations on assurance of such certifications, whether the (sub-)processor's technical or organisational measures, which had been the subject of certification audit, contribute to effectively ensuring the security of processing on behalf of the EU institution or body in accordance with Article 33 of the Regulation. However, certifications under international or industry standards, which assess processes and controls put in place within an organisation, do not constitute, in and of themselves, measures to supplement the relied-on transfer tool to effectively ensure an essentially equivalent level of protection.

Microsoft's compliance documentation, nor the measures identified in the Commission's 2021 DPIA address the main issues of the possession of the encryption keys and other information allowing Microsoft to re-identify natural persons, including by singling out, and of the processing of personal data in the clear.

479. The Commission also states that: "*Also, the immanent* [sic] *implementation of further stages of the EU Data Boundary Initiative is a measure that ensures the security of the processing operations. Moreover, new measures are implemented on a regular basis, for instance the roll-out of end-to-end encryption to protect all (video) calls in Teams.*"[852] Microsoft Ireland similarly refers to the EU Data Boundary and encryption in Teams, as additional measures.[853]

480. The EDPS has analysed the EU Data Boundary Initiative in paragraphs 330, 331 and 496 to 508. The EDPS has found that there are exceptions to and exclusions from the EU data Boundary and that transfers of personal data outside the EEA are to continue for largely the same purposes as before, e.g. support and security purposes, as well as Microsoft's business operations. The EDPS has seen no indications that the EU Data Boundary includes the implementation of effective supplementary measures. Yet such measures would have been required as regards recipients in the United States prior to the entry into force of the US adequacy decision, and likely would also be required as regards recipients in other third countries, such as China and India.

481. The EDPS addresses the roll out of end-to-end encryption for Teams calls in paragraphs 460 to 461, and double-key encryption envisaged by the Commission in paragraphs 456 to 459.

482. The EDPS notes that tools and measures that Microsoft Ireland has listed as measures that are "*aimed at protecting personal data by design*"[854] are not capable of preventing access, active or passive, by third-country public authorities to the transferred personal data. Microsoft Ireland does not allege that they would be capable of preventing such access, nor does it specify how any of these measures, separately or when used together, could have such capability. Therefore, they cannot be considered as supplementary measures.

Combination of supplementary measures

483. In their replies to the preliminary assessment, the Commission and Microsoft Ireland argue that the EDPS does not give proper weight to the effectiveness of the individual technical and organisational measures, especially when applied "*in conjunction or in parallel*".[855] In this regard, the Commission states that: "*The justifications provided [by*

[852] Commission's reply of 25 May 2023, para. 148.

[853] Reply by Microsoft Ireland of 26 May 2023, paras. 71 to 74 and 301 to 304, and Annexes 1 and 3, as well as Annex 12, pp. 6 and 8.

[854] Reply by Microsoft Ireland of 26 May 2023, paras. 52 and 53 and Annex 14 to 17. Those measures are: - Diagnostic Data Viewer, which enables customers to understand what diagnostic data Microsoft collects from client devices, privacy controls (which do not prevent the transmission of required service data); - Microsoft Priva and Purview tools, which aim to assist customers with data privacy compliance within the context of the features of these tools (risk and compliance assessment and management; privacy management); - Microsoft Cloud Policy Service for M365, which enables customers to configure and enforce policy settings (including security) for Microsoft 365 apps for enterprise on a user's device through the cloud; and - tools for customers to respond to data subject requests.

[855] Commission's reply of 25 May 2023, para. 149. See also reply by Microsoft Ireland of 26 May 2023, para. 285, 286 and 293.

the EDPS] for this conclusion are often limited to stating that an individual measure is not immune against being overcome, abstracted from any indicators of probability and severity of risk materialisation."[856]

484. The EDPS rejects these arguments. The EDPS has carefully examined all measures listed in the Commission's DPIA and in the replies by the Commission and Microsoft Ireland to the preliminary assessment. The EDPS considers that none have been effective in ensuring an essentially equivalent level of protection. The combination of ineffective supplementary measures cannot render such measures effective, as they do not fulfil all of the conditions for their effectiveness and thus do not compensate for the lack of protection in the third countries concerned. Crucially, the transfers correspond to use cases for which the EDPB has not been able to identify effective supplementary measures, in particular because the processing by the (sub-)processor requires personal data in the clear. Moreover, neither the Commission nor Microsoft Ireland substantiate specifically how a combination of ineffective supplementary measures would result in effectively ensuring an essentially equivalent level of protection.

Findings

485. None of the supplementary measures implemented on the reference date, either considered individually or combined, were effective in ensuring an essentially equivalent level of protection as required by the Regulation and the *Schrems II* judgment. The Commission's assessment of those measures in the transfer impact assessment it subsequently conducted was inadequate, particularly as it did not apply the EDPB's criteria for ensuring the application of effective supplementary measures and was not accompanied by an alternative but equally convincing assessment of the effectiveness of the supplementary measures.

486. Given that the Commission had no effective supplementary measures in place, and no satisfactory assurance that any even existed, in particular since the underlying situations fall under use cases 6 and 7 of EDPB Recommendations, its conclusion of the 2021 ILA, including SCCs,[857] was premature as it could not ensure appropriate safeguards under Article 48 of the Regulation. The Commission has therefore infringed Articles 46 and 48 of the Regulation.

Failure to request authorisation of the EDPS for the ad hoc contractual clauses for transfers. Violation of Articles 4(2), 46 and 48(1) and (3)(a) of the Regulation.

487. As noted in paragraph 245, an effective transfer tool ensuring an essentially equivalent level of protection as guaranteed in the EEA by the Regulation must be put in place by the Commission in order for it to allow transfers.

488. The 2021 ILA foresees that some data transfers in the context of the "*Core Online Services*" would fall within the scope of an adequacy decision.[858] The list of approved sub-processors in Attachment 4 to the DPA indicates that transfers may take place to Australia, Brazil, Canada, Chile, China, Egypt, Hong Kong, India, Israel, Japan, Malaysia,

[856] Commission's reply of 25 May 2023, para. 149.
[857] 2021 ILA, pp. 72-80.
[858] Section on "Data Transfers" in the body of the DPA, 2021 ILA, p. 38.

Republic of Korea, Serbia, Singapore, South Africa, Switzerland, the United Arab Emirates, the United Kingdom and the United States.

489. Any transfers to Canada, Israel, Japan, Republic of Korea, Switzerland and the United Kingdom would be covered by an adequacy decision as of the reference date until the adoption of this decision.[859] Following the entry into force of the US adequacy decision,[860] any transfers to the United States would also be covered by an adequacy decision.[861] This means that as of the reference date until the entry into force of the US adequacy decision, transfers to the United States had not been covered by an adequacy decision.

490. For all other transfers, including those to the United States prior to the entry into force of the US adequacy decision, the 2021 ILA foresees contractual safeguards, which included SCCs for transfers between the Commission and Microsoft Corporation.[862] Those SCCs were effectively replaced, under the 2021 ILA, when Microsoft Ireland and Microsoft Corporation concluded processor to processors SCCs[863] on 13 September 2021, i.e. after the reference date.[864]

491. In paragraphs 302 to 313, the EDPS has demonstrated the existence of direct transfers from the Commission to third countries, and in particular to the United States. Until 13 September 2021, the Commission relied for such transfers on the SCCs between the Commission and Microsoft Corporation. For reasons set out in paragraphs 244 and 245 of this decision, the Commission should have submitted such contractual clauses to the EDPS for authorisation in accordance with Article 48(3)(a) of the Regulation.

492. Individual *ad hoc* contractual clauses concluded pursuant to Article 48(3)(a) of the Regulation may in principle guarantee the existence of an essentially equivalent level of protection. The Commission may only use contractual clauses for transfers, however, if they guarantee the level of protection required by the Regulation, with or without the use of additional supplementary measures, as necessary. As explained in paragraph 251, the Commission could base its contractual clauses under Article 48(3)(a) of the Regulation on the SCCs for transfers under the GDPR, in particular the controller-processor transfer module, for transfers to Microsoft Corporation. The Commission would need to adapt them to reflect its nature as an EU institution and the requirements of the Regulation as explained in paragraphs 252 to 256, and to ensure that the Commission remains in control of the whole processing as explained in paragraphs 253 to 256, 258 and 259.

---

[859] See https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en. In so far as the scope of the transfers is covered by the respective adequacy decisions.

[860] Commission Implementing Decision EU 2023/1795 of 10 July 2023 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework (OJ L 231, 20.9.2023, p. 118).

[861] See https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en. In so far as the scope of the transfers is covered by the adequacy decision.

[862] 2021 ILA, pp. 72-80.

[863] See the Commission's additional reply of 7 June 2022, Annex 1, pp. 58-78. See also paras. 296, 299 and 303 of this decision.

[864] Microsoft Corporation had also concluded SCCs for transfers to its processors and sub-processors in third countries.

493. As explained in paragraph 491, the Commission should have submitted to the EDPS for authorisation the *ad hoc* contractual clauses under Article 48(3)(a) of the Regulation for transfers between the Commission and Microsoft Corporation. Instead, on 17 July 2020, Microsoft submitted a set of draft clauses for transfers "*from Microsoft (as data exporter) and Microsoft Corporation (as data importer)*" for the use of Microsoft Online Services by EU institutions and bodies to the EDPS for authorisation.[865] Those draft clauses were based on the SCC for transfers under Directive 95/46/EC. The EDPS held meetings with Microsoft and with the Commission in July and August 2020.[866] During those meetings, the EDPS informed them that before reviewing the clauses, the EDPS would need to receive concrete information on which personal data were being transferred for what purposes to which countries (or where the data could be accessed from). The EDPS also advised that the Commission as the controller would need to conduct what shortly after the meeting came to be known as 'transfer impact assessments', covering the jurisdictions to which the data are transferred.[867] The EDPS noted that based on the results of its transfer impact assessments, the Commission would need to appraise whether supplementary measures were needed to allow the transfers to continue.

494. It follows from the above that the Commission did not request the authorisation of the EDPS for transfers from it to Microsoft Corporation under Article 48(3)(a) of the Regulation. Moreover, Microsoft and the Commission did not pursue the request for authorisation to the EDPS of the *ad hoc* contractual clauses between Microsoft Ireland and Microsoft Corporation.

Finding

495. It follows, that the Commission concluded the SCCs for transfers of personal data from the Commission to Microsoft Corporation in the Commission's use of Microsoft 365[868] without having clearly mapped the proposed transfers, completed a transfer impact assessment, or included appropriate safeguards in those SCCs. Furthermore, it failed to obtain authorisation of those SCCs from the EDPS pursuant to Article 48(3)(a) of the Regulation. The Commission has therefore infringed Articles 4(2), 46 and 48(1) and (3)(a) of the Regulation.

EU Data Boundary

496. Microsoft first announced an initiative called "*EU Data Boundary for the Microsoft Cloud*" on 6 May 2021.[869] At that time, it pledged that this would enable both commercial and public sector customers in the EU "*to process and store all your data in the EU*" by the end of 2022.[870] The announcement stated that the commitment would apply "*across*

---

[865] See para. 285 of this decision.

[866] See para. 286 of this decision.

[867] The phrase 'transfer impact assessment' was coined a few weeks after the meeting, but accurately describes the assessment we advised would be necessary. The EDPS advised that the controller needed to be in a position to assess the level of data protection afforded by the applicable third-country laws and determine the possibility of putting in place additional contractual, technical and organisational safeguards to ensure an essentially equivalent level of protection to that afforded within the EU, as required by the Court of Justice in the *Schrems II* judgment.

[868] 2021 ILA, pp. 72-80.

[869] "Answering Europe's Call: Storing and Processing EU Data in the EU", May 6 2021, https://blogs.microsoft.com/eupolicy/2021/05/06/eu-data-boundary/

[870] "Answering Europe's Call: Storing and Processing EU Data in the EU", May 6 2021, https://blogs.microsoft.com/eupolicy/2021/05/06/eu-data-boundary/

all of Microsoft's core cloud services – Azure, Microsoft 365, and Dynamics 365".[871] It specified that: "*This plan includes any personal data in diagnostic data and service-generated data, and personal data we use to provide technical support.*"[872] Since then, Microsoft has specified these commitments, and in particular clarified exceptions and exclusions which allow the transfers of personal data to continue.

497. As explained in paragraphs 329 to 331, following its amendment of 19 December 2023, the 2021 ILA provides that:

> *"For EU Data Boundary Online Services (as defined in the Product Terms), Microsoft will store and process Customer Data within the European Union and EFTA, unless as provided for by documented exceptions set out in the Product Terms."*[873]

498. Under the Product Terms site, EU Data Boundary means "*Microsoft computers, computing environment, and physical data centers located solely in the European Union (EU) and the European Free Trade Association (EFTA)*".[874] An extensive and exhaustive list of EU Data Boundary Services appears on the same website.[875] As stated by Microsoft Ireland:

> "*The EU Data Boundary is a geographically defined boundary within which Microsoft has committed to store and process customer data for [Microsoft's] major commercial enterprise online services, including Azure, Dynamics 365, Power Platform, and Microsoft 365, subject to limited circumstances where customer data will continue to be transferred outside the EU Data Boundary.*"[876]

499. As further stated on the Product Terms site, the use of EU Data Boundary Services may result in various transfers of personal data, including customer data, diagnostic data, system-generated data,[877] and professional services data, outside the EU Data Boundary.[878] The Product Terms site lists 10 scenarios in which transfers are continuing for all EU Data Boundary services:
    a) remote access by Microsoft personnel to personal data stored and processed in the EU Data Boundary;
    b) customer-initiated data transfers, for example "*as part of service capabilities*" or in the context of "*fulfilling GDPR data subject rights requests worldwide*";
    c) transfers involving professional services data, which are provided to Microsoft by customers "*in the course of engaging with it for support or paid consulting services*";
    d) transfers related to protecting customers against global cybersecurity threats;

---

[871] "Answering Europe's Call: Storing and Processing EU Data in the EU", May 6 2021, https://blogs.microsoft.com/eupolicy/2021/05/06/eu-data-boundary/

[872] "Answering Europe's Call: Storing and Processing EU Data in the EU", May 6 2021, https://blogs.microsoft.com/eupolicy/2021/05/06/eu-data-boundary/

[873] Commission's email of 19 December 2023, Annex 2 (Amendment to Contract Documents), p. 3, point 5.

[874] Under the 2021 ILA, p. 3, the Product Terms site can be found at: https://www.microsoft.com/licensing/terms/product/PrivacyandSecurityTerms/EAEAS.

[875] https://www.microsoft.com/licensing/terms/product/PrivacyandSecurityTerms/EAEAS.

[876] Reply by Microsoft Ireland of 26 May 2023, para 71, Annex 7A, p. 1, and https://learn.microsoft.com/en-us/privacy/eudb/eu-data-boundary-learn. Website visited on 2 February 2024.

[877] The EDPS understands "system-generated data" as service generated data within the meaning of the 2021 ILA.

[878] https://learn.microsoft.com/en-us/privacy/eudb/eu-data-boundary-transfers-for-all-services. Website visited on 2 February 2024. Reply by Microsoft Ireland of 26 May 2023, Annex 7A,

e) transfers related to services in preview or trials;
f) transfers related to deprecated services;
g) transfers of personal data stored in on-premise software and client applications, including diagnostic data generated from use of such software and applications;
h) transfers of Entra Directory data, including username and email address;
i) transfers related to routing of customer traffic to reduce routing latency and maintain routing resiliency;
j) transfers related to Service and Platform Quality and Management.[879]

500. Moreover, the Product Terms site lists several scenarios where specific services transfer certain customer data or pseudonymised personal data, either "*on an ongoing basis*"[880] or temporarily,[881] and scenarios where optional service capabilities transfer such personal data.[882] In addition, certain services are excluded either permanently[883] or temporarily[884] from the EU Data Boundary.

501. With respect to the nature of the processing, Microsoft explains that to provide protection against security threats, it relies on "*advanced analytics capabilities, including artificial intelligence, to analyze aggregate security-related data, including activity logs, to protect against, detect, investigate, respond to, and remediate these attacks*".[885] It states that the processing is large-scale and preventative as well as responsive: "*The hyperscale cloud enables diverse, ongoing analysis of security-related data without prior knowledge of a specific attack.*" [886] The foregoing suggests that wide-ranging and granular records of

[879] https://learn.microsoft.com/en-us/privacy/eudb/eu-data-boundary-transfers-for-all-services. Website visited on 2 February 2024. See also reply by Microsoft Ireland of 26 May 2023, Annex 7A.
[880] https://learn.microsoft.com/en-us/privacy/eudb/eu-data-boundary-ongoing-partial-transfers. Website visited on 2 February 2024. See also reply by Microsoft Ireland of 26 May 2023, Annex 7A. **Scenarios include transfers of certain Microsoft 365 applications, Microsoft Teams and security services.**
[881] https://learn.microsoft.com/en-us/privacy/eudb/eu-data-boundary-temporary-partial-transfers. Website visited on 2 February 2024. See also reply by Microsoft Ireland of 26 May 2023, Annex 7A. **Scenarios include transfers of Exchange Online and Microsoft Teams, Windows Update and security services.**
[882] https://learn.microsoft.com/en-us/privacy/eudb/eu-data-boundary-transfers-for-optional-capabilities. Website visited on 2 February 2024. See also reply by Microsoft Ireland of 26 May 2023, Annex 7A. **Scenarios include transfers of a Microsoft 365 application, Microsoft Teams and security services.**
[883] https://learn.microsoft.com/en-us/privacy/eudb/eu-data-boundary-excluded-services. Website visited on 2 February 2024. See also reply by Microsoft Ireland of 26 May 2023, Annex 7A. **Among services excluded from EU Data Boundary are Microsoft 365 applications for builds pre-dating December 31 2022 and certain security services, such as Microsoft Defender**.
[884] https://learn.microsoft.com/en-us/privacy/eudb/eu-data-boundary-temporary-transfers-from-services. Website visited on 2 February 2024. See also reply by Microsoft Ireland of 26 May 2023, Annex 7A. **Among services temporarily excluded from EU Data Boundary are e.g. SharePoint and Viva Engage.**
[885] https://learn.microsoft.com/en-us/privacy/eudb/eu-data-boundary-transfers-for-all-services. Website visited on 2 February 2024. See also reply by Microsoft Ireland of 26 May 2023, Annex 7A.
[886] https://learn.microsoft.com/en-us/privacy/eudb/eu-data-boundary-transfers-for-all-services. Website visited on 2 February 2024. See also reply by Microsoft Ireland of 26 May 2023, Annex 7A.

users' activity containing various types of personal data[887] may be transferred, on a systematic and continuous/frequent basis, as input data for Microsoft's analytics.[888]

502. According to the Product Terms site, Microsoft has implemented measures to "*protect Customer Data*", including to respect the principles of data minimisation and purpose limitation.[889] In this regard, Microsoft states that it uses or relies on several measures of access control, such as "just-in-time" (JIT) access approvals and role-based access control (RBAC).[890] Microsoft further states that its personnel that have access to customer data operate from secure admin workstation (SAWs).[891] In addition, customers may establish additional access controls for "*many Microsoft cloud services*" by enabling Customer Lockbox.[892]

503. Moreover, Microsoft undertakes that its personnel may use either a secure admin workstation (SAW) or a virtual desktop infrastructure (VDI) to access pseudonymised personal data stored in the EU Data Boundary.[893] According to Microsoft, when a VDI is used, "*no data persists outside of the EU Data Boundary*" and the virtual machines are hosted on a physical machine located in the EU Data Boundary.[894]

504. The EDPS notes that even if storage of the personal data in third countries is avoided and the data remains in transit, this form of disclosure nonetheless constitutes a transfer.[895] Microsoft does not appear to dispute that the access is a transfer, as it referred to use of the VDI as a supplementary measure,[896] and supplementary measures

---

[887] See, in this respect, also the Dutch Ministry of Justice's DPIA of Office 365 ProPlus, 22 July 2019, pp. 22, 24, 25, 28, 32, 33, 39, 40, 68 to 70, 86, 89, 90 and 93. See also the Dutch Ministry of Justice's DPIA on Microsoft Teams, OneDrive, Sharepoint and Azure AD, 16 February 2022, pp. 9, 11, 32 to 34, 37 and 38 to 41. See similarly the findings of the Baden-Württemberg DPA's audit of Microsoft 365 in the context of a pilot project on its possible use in schools (23 April 2021, published 25 April 2022), in particular the analysis of the Baden-Württemberg DPA in annex 1 (pp. 5 and 6), annex 7 (pp. 89 and 92) and annex 10.

[888] See, in this respect, also the Dutch Ministry of Justice's DPIA of Office 365 ProPlus, 22 July 2019, pp. 22, 26, 28, 29, 32, 33 to 35 and 93. See also the Dutch Ministry of Justice's DPIA on Microsoft Teams, OneDrive, Sharepoint and Azure AD, 16 February 2022, pp. 9 to 11, 21, 27, 28, 31, 32, 37 to 38, 40, 43 to 45, 76, 77, 92, 93, 96, 105 and 108. See similarly the findings of the Baden-Württemberg DPA's audit of Microsoft 365 in the context of a pilot project on its possible use in schools (23 April 2021, published 25 April 2022), in particular the analysis of the Baden-Württemberg DPA in its opinion (pp. 8, 10 and 11), annex 1 (pp. 3 and 5 to 7), annex 7 (pp. 5, 36 to 96) and annex 10.

[889] https://learn.microsoft.com/en-us/privacy/eudb/eu-data-boundary-transfers-for-all-services. Website visited on 2 February 2024. See also reply by Microsoft Ireland of 26 May 2023, Annex 7A.

[890] https://learn.microsoft.com/en-us/privacy/eudb/eu-data-boundary-transfers-for-all-services. Website visited on 2 February 2024. See also reply by Microsoft Ireland of 26 May 2023, Annex 7A. According to RBAC, individual access is subject to strict requirements, such as the need-to-know principle, mandatory continual training, and oversight by one or more managers.

[891] https://learn.microsoft.com/en-us/privacy/eudb/eu-data-boundary-transfers-for-all-services. Website visited on 2 February 2024. See also reply by Microsoft Ireland of 26 May 2023, Annex 7A. SAWs are limited-function computers that reduce the risk of compromise from malware, phishing attacks, bogus websites, and pass-the-hash (PtH) attacks, among other security risks, and are enabled with countermeasures intended to make data exfiltration difficult.

[892] https://learn.microsoft.com/en-us/privacy/eudb/eu-data-boundary-transfers-for-all-services. Website visited on 2 February 2024. See also reply by Microsoft Ireland of 26 May 2023, Annex 7A.

[893] https://learn.microsoft.com/en-us/privacy/eudb/eu-data-boundary-transfers-for-all-services. Website visited on 2 February 2024. See also reply by Microsoft Ireland of 26 May 2023, Annex 7A.

[894] https://learn.microsoft.com/en-us/privacy/eudb/eu-data-boundary-transfers-for-all-services. Website visited on 2 February 2024. See also reply by Microsoft Ireland of 26 May 2023, Annex 7A.

[895] This is consistent with the EDPB's criteria of a transfer, which requires a controller or processor to disclose data by transmission or otherwise make it available to another controller or processor. See EDPB Guidelines 05/2021, section 2.2.

[896] Commission's additional reply of 7 June 2022, Annex 4, p. 11.

are only necessary in respect of transfers. The EDPS considers the VDI, like any form of access control, including usage of JIT and RBAC, to be a means of limiting transfers rather than an effective supplementary measure.[897]

505. In addition, according to the Product Terms site, Microsoft uses various techniques to pseudonymise personal data in system-generated logs, including encryption, masking, tokenisation, and data blurring.[898] However, as explained above, those measures are not effective when the Commission is not in sole possession of the cryptographic keys or where Microsoft has access to personal data in the clear or has access to other information that enables it to re-identify individuals, directly or indirectly.

506. Overall, EU Data Boundary represents a positive, incremental development that results in a greater proportion of the processing associated with the Commission's use of Microsoft 365 taking place in the EEA.

507. Nevertheless, the numerous exceptions and exclusions which cover customer data, service generated data, diagnostic data and professional services data demonstrate that transfers of personal data related to the Commission's use of Microsoft 365 outside the EEA continue to a significant extent. The evidence also suggests that large-scale bulk transfers also continue, to allow big-data analytics for security purposes to be carried out in the United States.

508. Moreover, the EDPS has seen no indications that the EU Data Boundary includes the implementation of effective supplementary measures. Yet such measures would have been required as regards recipients in the United States prior to the entry into force of the US adequacy decision, and likely would also be required as regards recipients in other third countries, such as China and India.

3.2.3. Findings

509. In view if the foregoing, the EDPS finds that the Commission, on the reference date and, except with regard to point b), second indent, and to point c),[899] continuously thereafter until the date of issuing this decision:

a) has infringed Article 29(3)(a) of the Regulation by failing to clearly provide in the 2021 ILA what types of personal data can be transferred to which recipients in which third country and for which purposes, and to give Microsoft documented instructions in that regard;

b) has infringed Articles 4(2), 46 and 48 of the Regulation by failing to provide appropriate safeguards ensuring that personal data transferred enjoy an essentially equivalent level of protection to that in the EEA since it:

- has not appraised, either prior to the initiation of the transfers or subsequently, what personal data will be transferred to which recipients in which third countries and for which purposes, thereby not obtaining the minimum information necessary to determine whether any

[897] See also paras. 430 to 434 of this decision.

[898] https://learn.microsoft.com/en-us/privacy/eudb/eu-data-boundary-learn. Website visited on 2 February 2024.

[899] With regard to point b), second indent, and point c), until the entry into force of the US adequacy decision.

supplementary measures are required to ensure the essentially equivalent level of protection and whether any effective supplementary measures exist and could be implemented;

- had not implemented effective supplementary measures for transfers to the United States taking place prior to the entry into force of the US adequacy decision, in light of the *Schrems II* judgment, nor has it demonstrated that such measures existed;

c) has infringed Articles 4(2), 46 and 48(1) and (3)(a) of the Regulation by:

- concluding the SCCs for transfers from the Commission to Microsoft Corporation[900] without having clearly mapped the proposed transfers, concluded a transfer impact assessment and included appropriate safeguards in those SCCs;

- failing to obtain authorisation of those SCCs for transfers from the Commission to Microsoft Corporation from the EDPS pursuant to Article 48(3)(a) of the Regulation;

d) has infringed Article 47(1) of the Regulation read in the light of Articles 4, 5, 6, 9 and 46 by failing to ensure that transfers take place "*solely to allow tasks within the competence of the controller to be carried out.*"

3.3. Unauthorised disclosures

3.3.1. Applicable law

510. Recital 20 of the Regulation states that:

> *"Personal data should be processed in a manner that ensures appropriate security and confidentiality of the personal data, including for preventing unauthorised access to or use of personal data and the equipment used for the processing and for preventing its unauthorised disclosure when it is transmitted."*

511. Recital 67 of the Regulation states that:

> *"Some third countries adopt laws, regulations and other legal acts which purport to directly regulate the processing activities of Union institutions and bodies. This may include judgments of courts or tribunals or decisions of administrative authorities in third countries requiring a controller or processor to transfer or disclose personal data, and which are not based on an international agreement in force between the requesting third country and the Union. The extraterritorial application of those laws, regulations and other legal acts may be in breach of international law and may impede the attainment of the protection of natural persons ensured in the Union by this Regulation. Transfers should only be allowed where the conditions of this Regulation for a transfer to third countries are met. This may be the case, inter alia, where disclosure is necessary for an important ground of public interest recognised in Union law."*

[900] 2021 ILA, pp. 72-80.

512. Recital 71 of the Regulation states that:

> *"When personal data moves across borders outside the Union it may put at increased risk the ability of natural persons to exercise data protection rights, in particular to protect themselves from the unlawful use or disclosure of that information."*

513. Article 4(1)(f) of the Regulation provides that personal data must be:

> *"processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')."*

514. Article 29(1), (3)(a) and (4) of the Regulation provides that:

> "1. Where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.
>
> *3. Processing by a processor shall be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the subject matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller. That contract or other legal act shall stipulate, in particular, that the processor:*
>
> *(a) processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by Union or Member State law to which the processor is subject; in such a case, the processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;*
>
> *4. Where a processor engages another processor for carrying out specific processing activities on behalf of the controller, the same data protection* obligations *as set out in the contract or other legal act between the controller and the processor as referred to in paragraph 3 shall be imposed on that other processor by way of a contract or other legal act under Union or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of this Regulation. Where that other processor fails to fulfil its data protection obligations, the initial processor shall remain fully liable to the controller for the performance of that other processor's obligations."*

515. Article 33(1) to (3) of the Regulation provides that:

> *"1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level*

of security appropriate to the risk, including, inter alia, as appropriate:

(a) the pseudonymisation and encryption of personal data;

(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

(c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

2. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

3. The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union law."

516. Article 36 of the Regulation provides that:

"Union institutions and bodies shall ensure the confidentiality of electronic communications, in particular by securing their electronic communications networks."

517. Article 49 of the Regulation provides that:

"Any judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data may only be recognised or enforceable in any manner if based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union, without prejudice to other grounds for transfer pursuant to this Chapter."

3.3.2. Analysis

Requirements of the Regulation as regards unauthorised disclosures of personal data processed in the EEA

518. Under Article 29(1) and (4) of the Regulation, an EU institution or body may only use processors and sub-processors providing sufficient guarantees to implement technical and organisational measures that the processing will meet the requirements of the Regulation and ensure the protections of the rights of the data subject. This means that processors and sub-processors that the EU institution or body considers using and that will process personal data in the EEA have to provide guarantees that they will not disclose the personal data to Member State or third-country authorities without instruction of the EU institution or body in accordance with EU law. Contractual safeguards reflecting these guarantees form a part of such organisational measures and

have to be included in the contract between controller and processor, and between processor and sub-processor.

519. Under Article 29(3)(a) of the Regulation, the contract between the controller and the processor must stipulate that the processor processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by EU or Member State law to which the processor is subject. If EU or Member State law requires the processor to process the data, it must inform the controller of that legal requirement before processing, unless that EU or Member State law prohibits it from doing so on important grounds of public interest.

520. As recognised by the EDPB, Article 29(3)(a) of the Regulation reveals the importance of the controller and processor carefully negotiating and drafting the processing agreement.[901] They may, for example, need to seek legal advice on the existence of legal requirements falling under Article 29(3)(a) of the Regulation.[902] The processor needs to do so in time to meet its obligation to inform the controller of such requirements before starting the processing.[903] In any event, any transfer or disclosure may only take place if authorised by EU law, including in accordance with Article 49 of the Regulation where applicable.[904]

521. The duty of the processor and any sub-processors to refrain from any processing activity not based on the controller's instructions also applies to transfers of personal data to a third country.[905] This includes refraining from transfers made to comply with disclosure requests from third-country authorities. The contract with the processor has to specify the requirements for transfers to third countries, taking into account the provisions of Chapter V of the Regulation.[906] This also includes specifying requirements and instructions as regards disclosure requests from third-country authorities.

522. In line with Articles 29(3)(a) and 30 of the Regulation, the EDPB recommends that controllers pay due attention to this specific point especially when the processor is going to delegate some processing activities to other sub-processors, and when the processor has divisions or units located in third countries. If the instructions by the controller do not allow for transfers or disclosures to third countries, the processor will not be allowed to assign the processing to a sub-processor in a third country, nor will the processor be allowed to have the personal data processed in one of its non-EU divisions.[907]

523. Under Article 29(4) of the Regulation, the same data protection obligations as set out in the contract between the controller and the processor have to be imposed on sub-processors through the contract between the processor and sub-processor, including the requirements and instructions as regards disclosure requests from third-country authorities.

524. Article 4(1)(f) of the Regulation sets out the principle of integrity and confidentiality which provides that personal data must be processed in a manner that ensures appropriate security of the personal data, including protection, inter alia, against

[901] See EDPB Guidelines 7/2020, para. 121.
[902] See EDPB Guidelines 7/2020, para. 121.
[903] See EDPB Guidelines 7/2020, para. 121.
[904] See EDPB Guidelines 7/2020, para. 121.
[905] In line with Articles 29(3)(a) and 30 of the Regulation. See EDPB Guidelines 7/2020, para. 119.
[906] See EDPB Guidelines 7/2020, para. 119.
[907] In line with Articles 29(3)(a) and 30 of the Regulation. See EDPB Guidelines 7/2020, para. 120.

unauthorised or unlawful processing. Such security must be ensured by using appropriate technical and organisational measures. This applies both to processing in and outside of the EEA. That principle is further developed in Articles 33 and 36 of the Regulation.

525. Under Article 33(1) of the Regulation, the controller and processor must implement appropriate technical and organisational measures, such as pseudonymisation and encryption, to ensure a level of security appropriate to the risk. In doing so, they must, inter alia, take into account the nature, scope, context and purposes of the processing, as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons. They must in particular take account of the risks presented from, inter alia, unauthorised disclosure of personal data, as provided in Article 33(2) of the Regulation.

526. Under Article 36 of the Regulation, EU institutions and bodies have an obligation to ensure the confidentiality of electronic communication, in particular by securing their electronic communications networks.

527. These provisions all entail that an EU institution or body must ensure that a processor or sub-processor engaged by it does not disclose personal data processed on behalf of that institution or body in an electronic communications network, unless the disclosure is expressly authorised by EU or Member State law.

528. Commitments in respect of Articles 4(1)(f), 33 and 36 of the Regulation have to be included in the contract between the EU institution and body and the processor and imposed also on sub-processors through processor-sub-processor contracts, as required by Article 29(1), (3) and (4) of the Regulation.

529. Extra-territorial application of third-country laws granting access to data processed by cloud service providers[908] poses a risk to effective compliance with the above-mentioned provisions of the Regulation. It poses such a risk not only in respect of personal data that have been or are being transferred to third countries but also of those processed solely in the EEA. Given the global nature of the infrastructure and resources of multinational or hyper-scale cloud service providers, access from other such jurisdiction is a foreseeable likelihood.

530. In this context, the EDPS recalls that EU institutions and bodies as controllers must ensure that personal data are not transferred or disclosed upon any judgment or decision of a third-country authority where such transfers or disclosures do not comply with EU law (Articles 46 and 48 of the Regulation) and are not authorised by it (Article 49 of the Regulation).

[908] E.g. the US CLOUD Act allows US law enforcement agencies to request access to data processed by cloud service providers subject to the jurisdiction of the US courts. This requirement is met for US-based companies and foreign companies falling within the US Supreme Court's understanding of "minimum contacts" with the US. Under the CLOUD Act, law enforcement access may be granted for data stored outside the US. Similarly, Section 702 FISA also applies extra-territorially. See the Memorandum on the Application of the CLOUD Act to EU Entities commissioned by the Dutch Ministry of Justice and Security (NCSC); the Rapport sur l'US CLOUD Act from the Federal department of justice and police of the Swiss Confederation; and Stephen Vladeck, Expert Opinion on the Current State of U.S. Surveillance Law and Authorities, commissioned by the Conference of German DPAs.

Essential equivalence of the protection of personal data transferred from EU institutions outside of the EEA. Existence of necessary protection against disclosure.

531. As clarified in the *Schrems II* judgment, data subjects whose personal data are transferred outside of the EEA under appropriate safeguards must be afforded a level of protection essentially equivalent to that which is guaranteed within the EEA.[909] This serves the objective of ensuring the continuity of the high level of protection afforded in the EEA where personal data are transferred to a third country.[910]

532. To comply with Article 46 of the Regulation, guarantees essentially equivalent to those under Article 29 of the Regulation have to be provided by the appropriate safeguards under Article 48 of the Regulation relied on for transfers between the EU institution or body as the controller and the processor and between the processor and sub-processors, if the EU institution or body has allowed transfers outside the EEA. Such guarantees have to cover requests for disclosure of personal data processed on behalf of the EU institution or body outside of the EEA.

533. Transfer tools such as those under Articles 48(2)(b) and (c) and 48(3)(a) of the Regulation[911] are based on contractual clauses[912] between the controller or processor transferring personal data, and the controller, processor or another recipient receiving those personal data in the third country or international organisation. Standard or *ad hoc* contractual clauses bind the signing entities to each other as regards the safeguards to be ensured for the processing of transferred personal data.[913] Those contractual clauses confer only contractual rights on data subjects against the entities that signed the clauses.[914] In view of their inherent contractual nature, standard or *ad hoc* contractual clauses cannot effectively counter deficiencies in the level of protection stemming from problematic legislation or practices[915] in the third country, in particular in relation to access by public authorities of that third country. Such clauses are not binding on public authorities as they are not party to the contract incorporating such clauses.[916]

534. The same limitation to the contractual clauses as regards public authorities applies also to transfer tools under Article 48(2)(d) of the Regulation,[917] which are based on unilateral or multilateral binding commitments undertaken within a corporate group in binding corporate rules or which are adhered to by controllers or processors in certification or codes of conduct.

535. Moreover, the EDPS stresses that the principle of integrity and confidentiality under Article 4(1)(f) of the Regulation is one the general principles of the Regulation that apply to all processing of personal data, including transfers. The specific practical requirements stemming from the general principles are concretised in obligations set out in other provisions of the Regulation. With regard to the principle of integrity and confidentiality, this has been concretised in obligations under Articles 33 and 36 of the Regulation. The EDPS therefore considers that the principle under Article 4(1)(f) of the

[909] *Schrems II* judgment, paras. 94 and 96.
[910] *Schrems II* judgment, para. 93. See also recital 6 GDPR.
[911] As well as transfer tools under Article 46(2)(c) and (d) and (3)(a) GDPR.
[912] Standard or *ad hoc* contractual clauses for transfers under the Regulation or the GDPR.
[913] See, to that effect, *Schrems II* judgment, paras. 56, 124 and 125, 133.
[914] See, to that effect, *Schrems II* judgment, paras. 56, 124 and 125, 133.
[915] See para. 264 of this decision.
[916] See, to that effect, *Schrems II* judgment, paras. 56 and 125.
[917] As well as transfer tools under Article 46(2)(b), (e) and (f) GDPR.

Regulation as developed in Articles 33 and 36 forms part of the essential equivalence of the level of protection that must be ensured when personal data are transferred outside the EEA.

536. The EU institution or body as the controller therefore has an obligation to put in place effective technical and organisational (including contractual) measures in accordance with Articles 4(1)(f), 29, 33 and 36 of the Regulation to ensure that the processing by processors and sub-processors meets the requirements of EU law and ensures the respect of the rights of the data subject. Such obligations must be reflected in the transfer tools under Article 48 of the Regulation.[918] An adequacy decision referred to in Article 47(1) of the Regulation does not set aside such obligations since they apply to any processing, including processing on behalf of the EU institution or body in a third country covered by an adequacy decision. Moreover, none of the adequacy decisions currently in force cover transfers of personal data processed in the EEA from a non-law enforcement entity to third country's law enforcement or national security authority.[919]

537. As required by Article 29(3)(a) of the Regulation, the processor must process personal data only on documented instructions from the EU institution or body as the controller, unless it is required to do so by EU or Member State law to which the processor is subject. In view of Articles 46 to 48 of the Regulation as interpreted (by analogy) in the *Schrems II* judgment, the EDPS considers that also third-country legislation may lawfully[920] require that the processor process personal data[921] which have been transferred to that third country, subject to the following condition. Such third-country legislation to which the processor is subject must respect the essence of the fundamental rights and freedoms recognised by the Charter and must not exceed what is necessary and proportionate in a democratic society to safeguard one of the important objectives as also recognised in EU or Member State law, such as those listed in Article 25(1) of the Regulation.[922] [923]

538. Article 29(3)(a) of the Regulation further provides that where the processor is required to process personal data by EU or Member State law to which it is subject, the processor must inform the controller of that legal requirement before processing, unless that law prohibits providing such information on important grounds of public interest.

539. To ensure a level of protection essentially equivalent to that afforded by Article 29(3)(a) of the Regulation, in the absence of an adequacy decision, relevant appropriate safeguards must be provided in the transfer tool. Such safeguards include an obligation of the processor to notify the controller of any disclosure request by a third-country authority. They also include an obligation of the processor to review the legality of such a request and to challenge the request if there are reasonable grounds that the request

[918] As well as transfer tools under Article 46 GDPR.
[919] See in this respect annex to the EDPB-EDPS Joint Response to the LIBE Committee on the impact of the US Cloud Act on the European legal framework for personal data protection, p. 3, available at: https://edps.europa.eu/data-protection/our-work/publications/opinions/edpb-edps-joint-response-us-cloud-act_en.
[920] I.e. in compliance with the Regulation.
[921] Within the meaning of Article 29(3)(a) of the Regulation.
[922] See *Schrems II* judgment, paras. 141, 174 and 187, EDPB Recommendations 01/2020, para. 38, and EDPB Recommendations 02/2020, paras. 22 and 24.
[923] This is without prejudice to obligations stemming from other EU law that governs processing of personal data, including transfers, in particular in the law enforcement and national security contexts.

is unlawful. An example of such guarantees is provided in Clause 15 of the SCCs set out in Implementing Decision (EU) 2021/914.

540. In view of the foregoing, third-country legislation may lawfully[924] prohibit the controller from being informed of the disclosure request in this regard where the condition referred to in paragraph 537 is met.

541. In this regard, the EDPS stresses that, in the absence of an adequacy decision, the controller must carry out a transfer impact assessment before initiating any transfers (assessing whether the third-country legislation meets the condition set out in paragraph 537). The EU institutions and bodies should look to EDPB Recommendations 01/2020 and 02/2020 for guidance in assessing whether legislation and practices of a third country fulfil European essential guarantees as regards access and disclosure requests by its public authorities.[925] Such an assessment requires, inter alia, that the controller become aware of any applicable third-country legislation that requires that the processor processes transferred personal data and of legislation that may prevent the controller from being informed of such processing. This allows the controller to ascertain whether any such legislation exceeds what is necessary and proportionate in a democratic society to safeguard one of the important objectives as also recognised in EU or Member State law, such as those listed in Article 25(1) of the Regulation. Without such an assessment, the controller cannot satisfy itself that the guarantees provided in the transfer tool will ensure an essentially equivalent level of protection. It follows that without such an assessment, the controller must not initiate or continue with transfers as further demonstrated in section 3.2.2.3.

542. Where it is ascertained, following the performance of a transfer impact assessment, that the third-country legislation or practices[926] prohibit the processor or sub-processor from notifying the EU institution or body as a controller or challenging a disclosure request, the EU institution or body must be satisfied that the condition referred to in paragraph 537 is met.

543. In this regard, the EDPS stresses that the confidentiality of communications, in particular, must not be compromised because of problematic third-country legislation and practices. The requirement of confidentiality forms part of the protection of personal data processed by EU institutions and bodies in the EU legal order. The EU institutions and bodies need to ensure the continuity of such protection to personal data transferred outside of the EEA.

Effective technical and organisational measures to prevent unauthorised disclosures

544. Effective protection against problematic legislation or practices may be provided by international commitments that the third country has accorded to the EU institution or body[927] and enacted in the third country's legislation. Those commitments must be binding on the public authorities in that third country and not rendered ineffective by

[924] I.e. in compliance with the Regulation.
[925] See e.g. paras. 40 to 42 of EDPB Recommendations 01/2020 and chapter 3 of EDPB Recommendations 2/2020.
[926] See also paras. 263 to 265 of this decision.
[927] In accordance with the customary privileges, immunities and facilities accorded to international organisations by international public law.

the concurrent application of the public authorities' other obligations.[928] Binding and effective international commitments that a third country made to the EU or EU institutions and bodies in respect of protecting data, including personal data, transferred by the EU institution or body or on its behalf could mean that such (personal) data are considered privileged information. It could also mean that the EU institution or body is a privileged sender and the processor or sub-processor possibly a privileged recipient. Such binding and effective international commitments could therefore allow such transfers to fall under use case 4[929] of EDPB Recommendations 1/2020, even in situations where the processing by the recipient requires access to personal data in the clear.

545. Moreover, the EU institutions and bodies may ensure effective protection against problematic legislation or practices also by supplementing contractual safeguards and measures and organisational measures with effective technical measures. Such technical measures must prevent access to personal data outside the EEA by the public authorities of a third country with problematic legislation or practices.[930] Only then can the EU institution or body guarantee a level of protection essentially equivalent to that which is guaranteed in the EEA, as required by Articles 4(1)(f), 26, 29 33, 36, 46 and 48 of the Regulation.

546. Articles 46 and 48 of the Regulation as interpreted in the *Schrems II* judgment require that if, prior to any transfer, including onward transfer, the EU institution or body has reason to believe that problematic legislation or practices exist, it must not initiate or continue with the transfer,[931] unless it has put in place effective supplementary measures.

3.3.2.1. Unauthorised disclosures under the 2021 ILA

547. The provisions on disclosure in the DPA are broad in scope. They encompass both the processing undertaken by Microsoft to provide the online services and processing it carries out for the purposes of its own business operations.[932] The provisions contain a number of qualifications and limitations, as the EDPS analyses below.[933]

548. On 19 December 2023, the Commission and Microsoft concluded an amendment to the DPA which, inter alia, amended the first paragraph in the section "Disclosure of Processed Data" and added a new, seventh paragraph in that section:

---

[928] See by analogy paras. 134 and 214 of the Opinion 1/15 (*EU-Canada PNR Agreement,* ECLI:EU:C:2017:592) and paras. 74 and 75 of the Schrems I judgment (*Schrems*, C-362/14, ECLI:EU:C:2015:650).

[929] See para. 276 of this decision.

[930] *Schrems II* judgment, paras. 134 and 135.

[931] See in particular paras. 140 to 146 of the *Schrems II* judgment. See also Clause 14 of the SCCs set out in Implementing Decision (EU) 2021/914.

[932] Sections on '*Nature of Data Processing Ownership*' and '*Disclosure of Personal Data*' in the DPA, 2021 ILA, pp. 28 and 29.

[933] In addition, German data protection authorities have found in their assessment of Microsoft 365 similar limitations and qualifications of provisions on disclosures in the September 2022 Data Processing Agreement. See in this respect the findings of the Conference of German DPAs on Microsoft Online Services (Microsoft 365), 24 November 2022, in summary (p. 5) and assessment (p. 27 to 38). See also the findings of the Baden-Württemberg DPA's audit of Microsoft 365 in the context of a pilot project on its possible use in schools (23 April 2021, published 25 April 2022), in particular in the Baden-Württemberg DPA's opinion (pp. 18 and 19). As have other data protection authorities, such as the Cypriot and Greek. See in this respect the EDPB report on the 2022 Coordinated enforcement action on the use of cloud-based services by the public sector, 17 January 2023, in report (pp. 18 and 32) and in particular findings of the Cypriot and Greek DPAs in annex (pp. 16, 17, 55 and 56).

> *"Microsoft and/or its Subprocessors shall not give access to or disclose any Processed Data processed on behalf of the Customer, actively or passively, intentionally or unintentionally, to any Member State authority, third country authority, international organisation or other legal or natural person (collectively referred to as "third parties"), including transfers of personal data resulting from such disclosure, unless the conditions laid down in the EUDPR for such disclosure are met. For purposes of this section, "Processed Data" means: (a) Customer Data; (b) Personal Data; and (c) any other data processed by Microsoft in connection with the Online Service that is Customer's confidential information. For the avoidance of doubt, the Parties do not expect or plan for such unauthorized transfers to take place in the context of the execution of the ILA.*
>
> *Microsoft will only disclose or provide access to any Processed Data as required by law (and subject to the provisions of this section) and provided that the laws and practices respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society and, as applicable, to safeguard one of the objectives listed in Article 23(1) of GDPR or Art. 25(1) EUDPR."* (emphasis as included in the original text of the amendment marks parts that are new or changed compared to the previous version of the DPA)[934]

Insufficient warranties provided as regards disclosures of personal data in view the required assessment of third-country legislation. Violation of Articles 4(1)(f), 33(1) and (2) and 36 of the Regulation

549. Article 4(1)(f) of the Regulation sets out the principle of integrity and confidentiality which provides that personal data must be processed in a manner that ensures appropriate security of the personal data, including protection, inter alia, against unauthorised or unlawful processing. Such security must be ensured by using appropriate technical and organisational measures. This applies both to processing in and outside of the EEA.

550. Under Article 33(1) of the Regulation, the controller and processor must implement appropriate technical and organisational measures, to ensure a level of security appropriate to the risk. In doing so, they must, inter alia, take into account the risks presented by processing, in particular from unauthorised disclosure of personal data, as provided in Article 33(2) of the Regulation. Furthermore, the EDPS considers that implementing such measures is a necessary pre-condition for ensuring the confidentiality of electronic communications in accordance with Article 36 of the Regulation.

551. Following its amendment of 19 December 2023, the DPA provides that:

> *"Microsoft and/or its Subprocessors shall not give access to or disclose any Processed Data processed on behalf of the Customer, actively or passively, intentionally or unintentionally, to any Member State authority, third country authority, international organisation or other legal or natural person (collectively referred to as "third parties"), including transfers of personal data resulting from such disclosure, unless the conditions laid down in the EUDPR for such disclosure are met.* [935]

[934] Commission's email of 19 December 2023, Annex 2 (Amendment to Contract Documents), p. 2.
[935] 2021 ILA, pp. 29.

Microsoft will only disclose or provide access to any Processed Data as required by law (and subject to the provisions of this section) and provided that the laws and practices respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society and, as applicable, to safeguard one of the objectives listed in Article 23(1) of GDPR or Art. 25(1) EUDPR."[936]

552. With regard to these provisions of the DPA, the EDPS notes that in view of their inherent nature, any contractual warranties cannot effectively counter deficiencies in the level of protection stemming from problematic legislation or practices in the third country, in particular in relation to access by public authorities of that third country. Moreover, such clauses are not binding on public authorities as they are not party to the contract incorporating such clauses.[937]

553. It follows that in order to ensure the protection against unauthorised disclosures, as required by Articles 4(1)(f) and 33 of the Regulation, providing contractual warranties cannot suffice without having conducted the assessment necessary to ensure that such warranties are respected in practice, including in relation to public authorities.[938] The Commission as the controller must satisfy itself that the third-country legislation to which the processor is subject respects the essence of the fundamental rights and freedoms recognised by the Charter and does not exceed what is necessary and proportionate in a democratic society to safeguard one of the important objectives as also recognised in EU or Member State law, such as those listed in Article 25(1) of the Regulation.[939]

554. However, as demonstrated in paragraphs 377 to 414, on the reference date the Commission had not carried out a transfer impact assessment for transfers of personal data outside the EEA in the context of its use of Microsoft 365. Moreover, the Commission's transfer impact assessment carried out after the reference date did not assess the level of protection in all third countries to which transfers of personal data are envisaged under the 2021 ILA in the Commission's use of Microsoft 365. Nor did it properly assess the level of protection in the United States as regards transfers prior to the entry into force of the US adequacy decision.

555. In doing so, the Commission has failed to assess whether the legislation of all third countries to which personal data are envisaged to be transferred under the 2021 ILA and whose public authorities may make disclosure requests meets the condition referred to in paragraph 553. Given that the contractual warrantees cannot ensure the protection against unauthorised disclosures where the legislation does not meet the condition referred to in paragraph 553, the Commission has failed to ensure that Microsoft and its sub-processors do not make disclosures of personal data processed on behalf of the Commission within and outside of the EEA, that are not authorised under EU law.

556. The Commission has therefore failed to ensure the protection against unauthorised disclosures, as required by Article 4(1)(f) of the Regulation. It has also failed to implement appropriate organisational measures to ensure an appropriate level of

---

[936] Commission's email of 19 December 2023, Annex 2 (Amendment to Contract Documents), p. 2.

[937] See, to that effect, *Schrems II* judgment, para. 125.

[938] See, in this respect, also Clause 14(b)(ii) of the SCCs between Microsoft Ireland and Microsoft Corporation of 13 September 2021

[939] This is without prejudice to obligations stemming from other EU law that governs processing of personal data, including transfers, in particular in the law enforcement and national security contexts.

security which must take into account risks that are presented by unauthorised disclosure of personal data as required by Article 33(1) in (2) of the Regulation. In doing so, the Commission has also failed to ensure the confidentiality of electronic communications as required by Article 36 of the Regulation.

557. With regard to Article 36, the Commission states that:

> "*An unauthorised disclosure of Commission data by Microsoft would not be an act of communication by the Commission itself, neither would Microsoft use the Commission's communication networks. No statement of the EDPS gives reason to doubt that the electronic communication networks of the Commission would not be secured. Any electronic communication with Microsoft takes places via public network connections, protected by robust encryption. Therefore, the EDPS' allegation on a possible infringement of Article 36 of the Regulation is unsubstantiated and speculative.*"[940]

The EDPS rejects these arguments.

558. First, Article 36 of the Regulation provides that EU institutions and bodies must ensure the confidentiality of electronic communications. The Regulation does not limit that obligation to the electronic communications of the EU institutions and bodies.[941] The EDPS therefore considers that this provision includes all electronic communications transmitted or stored in the context of processing that is carried out by the Commission or on its behalf.[942] The Commission as a controller must ensure and be able to demonstrate compliance with Article 36 in view of the accountability principle set out in Articles 4(2) and 26 of the Regulation.

559. Second, Article 36 of the Regulation indeed further provides, in a non-exhaustive manner, that EU institutions and bodies must ensure the confidentiality of electronic communications, in particular by securing their electronic communications networks. However, it cannot be concluded on that basis that the reference to the electronic communications networks of the EU institutions and bodies implies that Article 36 circumscribes its effects to the electronic communications of EU institutions and bodies. Quite the opposite, since there is a clear distinction in Article 36 of the Regulation between "their electronic communications networks" and "electronic communications". Moreover, securing their electronic communications networks is just one of the ways in which the EU institutions and bodies must ensure the confidentiality of electronic communications. In this regard, the EDPS also clarifies that it does not find that the Commission's electronic communication networks are not secured.

560. Pursuant to Article 49 of the Regulation, if a third-country authority requires the transfer or disclosure of personal data processed under the 2021 ILA, the Commission, Microsoft and its sub-processors may only carry out the transfer or disclosure if the third-country authority's decision is based on an international agreement between the third country and the EU.[943] In this regard, the EDPS considers that "*without prejudice*

---

[940] Commission's reply of 25 May 2023, para. 172.
[941] As it could have by e.g. providing "**their** electronic communications".
[942] The EDPS notes, however, that Article 36 of the Regulation covers information included in electronic communications, irrespective of whether such information constitutes personal data.
[943] See also Article 48 of the GDPR and the EDPB-EDPS joint response to the LIBE Committee on the impact of the US Cloud Act on the European legal framework for personal data protection.

to other grounds for transfer pursuant to [Chapter V]" as provided in Article 49 of the Regulation does not imply that compliance with that Article is unnecessary where there is another ground for transfer under Chapter V,[944] but rather that Article 49 constitutes an additional condition that must be met in case a transfer or disclosure is requested by a third-country court, tribunal or administrative authority. This requirement applies to personal data processed within and outside the EEA. It is not reflected in the 2021 ILA. On the contrary, as analysed in preceding section, the 2021 ILA's provisions fail to ensure that Microsoft and its sub-processors do not make disclosures in breach of EU law. By concluding such a contract, the Commission has made it possible that were these disclosures in breach of EU law to occur, they would infringe Article 49 of the Regulation.

Ineffective technical and organisational measures to prevent unauthorised disclosures. Violation of Articles 4(1)(f), 33(1) and (2) and 36 of the Regulation

561. As noted above, the controller must ensure protection, inter alia, against unauthorised or unlawful processing, as required by Article 4(1)(f) of the Regulation. Moreover, the controller and processor must implement appropriate technical and organisational measures, including pseudonymisation and encryption, to ensure a level of security appropriate to the risk, as required by Article 33(1) of the Regulation. In doing so, they must, inter alia, take into account the risks presented by processing, in particular from unauthorised disclosure of personal data, as provided in Article 33(2) of the Regulation. Implementing such measures is a necessary pre-condition for ensuring the confidentiality of electronic communications in accordance with Article 36 of the Regulation.

562. As explained in paragraphs 554 and 555, the Commission has failed to assess whether the legislation of all third countries to which personal data are envisaged to be transferred under the 2021 ILA and whose public authorities may make disclosure requests meets the condition referred to in paragraph 553.

563. As explained in paragraph 545, the Commission could remedy such failure also by supplementing contractual safeguards and measures and organisational measures with effective technical measures. Such technical measures must prevent access to personal data processed within and outside of the EEA by public authorities of a third country whose legislation does not meet the condition referred to in paragraph 553.

564. The Commission has relied on technical and organisational measures, such as encryption, pseudonymisation and access control solutions provided by Microsoft also to protect against unauthorised disclosures of personal data. However, as demonstrated in paragraphs 415 to 486 of this decision,[945] these measures are not effective in preventing unauthorised disclosures.[946] Microsoft retains access to the personal data processed in the clear. Where personal data are encrypted, Microsoft controls the implementation of the encryption algorithms and infrastructure and it still retains access to the cryptographic keys. [947] The Commission's implementation of DKE solution is limited to sensitive non-classified information. Also, the EDPS cannot take a view on

[944] As suggested by the Commission in its reply of 25 May 2023, para. 164.
[945] See paras. 415 to 486 of this decision.
[946] See, in this respect, similarly the findings of the Conference of German DPAs on Microsoft Online Services (Microsoft 365), 24 November 2022, in summary (p. 7) and assessment (p. 37, 38, 54 to 57).
[947] See paras. 435 to 454 of this decision.

its effectiveness as a supplementary measure in the cases where it is deployed.[948] The Commission should also assess effectiveness of any end-to-end encryption solution implemented for Teams calls as a supplementary measure.[949] Microsoft controls how and where personal data are pseudonymised and has additional information that would allow re-identification, including by singling out, of individuals from pseudonymised data.[950] The 'Customer Lockbox' access control solution is not designed to distinguish and prevent access to personal data resulting from orders or requests from third-country public authorities. Neither are the Just-In-Time, secure admin workstations, role-based access controls and other access and logging measures.[951]

565. The implemented technical and organisational measures, either considered individually or combined, do not ensure that processing takes place in accordance with the Regulation and in particular with the principle of integrity and confidentiality within the EEA and, as part of an essential equivalence of the level of protection, also outside of the EEA. The Commission's failure to implement effective technical and organisational measures therefore results in a breach of Articles 4(1)(f), 33 and 36 of the Regulation.

566. The Commission has therefore failed to implement appropriate technical and organisational measures to ensure an appropriate level of security which must take into account risks that are presented by unauthorised disclosure of personal data as required by Article 33(1) in (2) of the Regulation. In doing so, the Commission has also failed to ensure the protection against unauthorised disclosures, as required by Article 4(1)(f) of the Regulation and to ensure the confidentiality of electronic communications as required by Article 36 of the Regulation.

567. In its reply to the preliminary assessment, Microsoft Ireland states that:

> *"In addition, Microsoft has stated clearly in its White Papers that 'Microsoft* ***does not provide, and has never provided, EU public sector customer data to any government[5]*** *(Annex 2) and it commits to challenging every government request for access to data where there is a lawful basis for doing so. Contrary to the EDPS' preliminary findings, Microsoft has also committed 'not to provide any third party: (a) direct, indirect, blanket, or unfettered access to customer data; (b) platform encryption keys used to secure customer's data or the ability to break such encryption; or (c) access to customer's data if Microsoft is aware that the data is to be used for purposes other than those stated in the third party's request.' (Annex 2) These are all highly far-reaching commitments which, to Microsoft's knowledge, no other comparable service provider has offered.*
>
> *[5] [footnote 5]* ***For clarity, under U.S. law, providers can neither confirm nor deny having received any specific legal demands subject to a secrecy obligation.*** *While* ***Microsoft is obligated to comply with these restrictions in U.S. law****, we disagree with them and continue to advocate for changes in the law to provide our customers and the public additional, important transparency. Please see our biannual U.S. National Security Report for the most comprehensive, legally permissible picture we can provide at this point of national security-related requests*

[948] See paras. 456 to 459 of this decision.
[949] See paras. 460 and 461 of this decision.
[950] See paras. 462 to 468 of this decision.
[951] See paras. 430 to 434 of this decision.

we receive from the U.S. government." (emphasis added)[952]

"In this regard, as set out in para. 76, ***Microsoft states, in relation to the US and other non-adequate third countries which it (onward) transfers personal data that it does not provide and has never provided EU public sector customer data to any government****:*

'Microsoft is committed to defending the principle that governments should never place global technology providers in the middle of state-on-state surveillance, and Microsoft does not provide, and has never provided, EU public sector customer data to any government'[158]*.*

[158] *See* ***footnote 5****.*

In addition, ***Microsoft continuously issues ad hoc confirmations of non-disclosure to the Commission, upon request****." (emphasis added)*[953]

"The ***Additional Safeguards Addendum must in particular be viewed in combination with Microsoft's important statements that it 'does not provide, and has never provided, EU public sector customer data to any government'***[167] *and also the EU Data Boundary, by which most customer data (which generally could be viewed as more easily triggering redress) is not transferred outside the EU.*

[167] *See Transfers White Paper, p. 5 and 12 (Annex 2) and* ***footnote 5****."(emphasis added)*[954]

"In particular in relation to Microsoft, it should be emphasized that Microsoft does not receive a large number of disclosure requests generally. Indeed, ***Microsoft has not received any US civil legal requests seeking the European Commission's customer data or personal data. And, as detailed above, 'Microsoft does not provide, and has never provided, EU public sector customer data to any government'***[168]*. This is all highly relevant information that the EDPS fails to take into account as it has not done a concrete assessment.*

[168] *See* ***footnote 5****."*[955] *(emphasis added)*

568. At the hearing of 23 October 2023, Microsoft Ireland has stated that "*Microsoft can confirm that less than 1% of the disclosure requests received by Microsoft are for enterprise, as opposed to individual customers*".

569. The EDPS takes note of the transparency statements quoted in paragraphs 567 and 568. The EDPS, however, considers that such statements offer a significantly qualified and therefore limited evidential value, in particular in light of any obligation, under legislation to which Microsoft is subject, which prohibits Microsoft, its affiliates and sub-processors from confirming or denying any specific legal demands subject to a secrecy obligation.[956] This is also relevant with regard to the statement made by the Commission in its reply to the preliminary assessment.[957] In that statement, the

[952] Reply by Microsoft Ireland of 26 May 2023, para. 25, and similarly para. 76, in which Microsoft Ireland refers to the Transfers White Paper (Annex 2 of its reply) describing "*additional important transparency in relation to government access*".

[953] Reply by Microsoft Ireland of 26 May 2023, para. 273.

[954] Reply by Microsoft Ireland of 26 May 2023, para. 300.

[955] Reply by Microsoft Ireland of 26 May 2023, para. 310.

[956] Such as the obligation under US law cited by Microsoft Ireland: "*providers can neither confirm nor deny having received any specific legal demands subject to a secrecy obligation*" (see para. 567 of this decision).

[957] Commission's reply to the preliminary assessment of 25 May 2023, para. 166.

Commission claims that the EDPS' assumption of risks for extra-territorial application of third-country law for processing operations carried out solely in the EU is "*purely hypothetical*" as there are no indications that Microsoft has provided personal data in response to requests from third-country authorities. Given that Microsoft is prohibited from confirming or denying any specific legal demands subject to a secrecy obligation,[958] there cannot be any specific indications. In fact, given such third-country legislation, the risk is not hypothetical but actually foreseeable.

570. 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.[959]

571. Transparency reports can serve as a reliable source of information to assess third-country laws and practices on the condition that they expressly and unreservedly confirm the fact that no access requests were received. Transparency reports that are merely silent on this point would not qualify as sufficient evidence as crucial information may be omitted. Moreover, such reports most often focus on access requests received from law enforcement authorities and hence fail to provide figures on access requests received for national security purposes. Any omission of this information may therefore imply that relevant information cannot be shared, and not that no access requests have been received.[960]

Failures in notification of disclosure requests. Violation of Article 29(3)(a) of the Regulation

572. Under the DPA, the obligation of Microsoft and its sub-processors to notify the Commission of a disclosure request is conditional. It applies only if the law applicable to the requesting third party permits notification.[961] The DPA further provides that Microsoft and its sub-processors will use their best efforts to obtain a waiver of any prohibition of such notification under that law.[962]

573. Until 13 September 2023, this qualified commitment to notify the Commission was reproduced in substance in the SCCs[963] applicable between the Commission and Microsoft Corporation and in the Additional Safeguards Addendum appended to those SCCs.[964] On 13 September 2023, Microsoft Ireland and Microsoft Corporation concluded processor to processor SCCs on the basis Implementing Decision (EU) 2021/914 which effectively replaced the SCCs between the Commission and Microsoft Corporation and were subsequently incorporated in the 2021 ILA.[965] According to the Commission, further transfers are carried out "*pursuant to sub-processor agreements between Microsoft Corp. and its sub-processors in accordance with the SCCs in place.*"[966]

---

[958] Microsoft affiliates and sub-processors may also be subject to such obligations.
[959] See EDPB Recommendations 01/2020, paras. 135 and 136.
[960] See EDPB Recommendations 01/2020, para. 47 and Annex 3.
[961] Section on '*Disclosure of Personal Data*' in the DPA, 2021 ILA, p. 30, first para.
[962] Section on '*Disclosure of Personal Data*' in the DPA, 2021 ILA, p. 30, second para.
[963] Clause 5(d)(i) of the SCCs, 2021 ILA, p. 74.
[964] Clause 1(b) of the Additional Safeguards Addendum, 2021 ILA, p. 79.
[965] See paras 296, 299 and 303 of this decision.
[966] Commission's substantive reply of 15 October 2021, para. 2.7.12, p. 18.

574. Clause 15[967] of the processor to processor SCCs provides for obligations on Microsoft Corporation as the data importer to notify Microsoft Ireland as the data exporter if it receives a legally binding disclosure request or if it becomes aware of any direct access by public authorities to the transferred personal data. It also provides that Microsoft Ireland must forward such notification to the Commission as the controller. Similarly to the DPA, Clause 15 further provides that where Microsoft Corporation is prohibited from notifying Microsoft Ireland under *the laws of the third country to which data have been transferred*, it is to use its best efforts to obtain a waiver of such prohibition.

Disclosure requests pertaining to personal data in the EEA

575. As noted in paragraph 519, Article 29(3)(a) of the Regulation provides that only EU or Member State law to which the processor is subject may lawfully[968] prohibit, on important grounds of public interest, the controller from being informed of the request for disclosure of personal data processed in the EEA.

576. Under the DPA, *the law applicable to the requesting third party* may prohibit Microsoft and its sub-processors from notifying the Commission of a request for disclosure made by that third party of any "*processed data*" processed on behalf of the Commission. It follows that, according to the DPA, for personal data processed in the EEA, Microsoft and its sub-processors may be prohibited *by third-country law* from informing the Commission of a request made by a third-country public authority for disclosure. The Commission has thus failed to provide that only EU or Member State law to which Microsoft or its (sub-) processor is subject may prohibit notification in question. This is in breach of Article 29(3)(a) of the Regulation.

577. In its reply to the preliminary assessment, the Commission states that Chapter V of the Regulation, and in particular Article 49, would apply in any event.[969] It further states that:

> *"[Article 49 of the Regulation] reassures [it] that, if a third-country authority requires the transfer or disclosure or personal data processed under the ILA, Microsoft Ireland will not transfer/disclose that data unless the conditions of [that Article] are fulfilled. By requiring additional reassurances to be contractually agreed between the Commission and Microsoft Ireland, the EDPS essentially implies that Article 49 of the Regulation and Article 48 GDPR are ineffective, which the Commission certainly does not agree with."*[970]

The EDPS welcomes this statement and expects that the Commission and its (sub-)processors fully comply with Article 49 of the Regulation when they receive a judgment or administrative decision issued in a third country requiring a transfer or disclosure of personal data. The EDPS, however, cannot comprehend why the Commission seems to suggest that Article 49 of the Regulation need not always be complied with, as its interpretation of the words "*without prejudice to other grounds for transfer pursuant to [Chapter V]*" would lead to conclude.[971] Moreover, the EDPS has been clearly contesting the compliance of the provisions of the DPA, in so far as they allow third-country legislation to prohibit notification of a request for disclosure of

[967] Reply by Microsoft Ireland of 26 May 2023, Annex 1B, pp. 11 and 12.
[968] I.e. in compliance with the Regulation.
[969] Commission's reply of 25 May 2023, para. 161.
[970] Commission's reply of 25 May 2023, para. 162.
[971] Commission's reply of 25 May 2023, para. 164.

personal data processed in the EEA to the Commission, with the requirements of Article 29(3)(a) of the Regulation. Compliance with Article 29(3)(a) of the Regulation entails that the instructions provided by the controller do not contradict applicable EU law, which includes Article 49 of the Regulation. In any event, the Commission is not exempt from its obligations under Article 29(3)(a) simply because it declares that its processor complies with Article 49 of the Regulation. The argument of the Commission must therefore be rejected as it does not demonstrate compliance with Article 29(3)(a) of the Regulation.

Disclosure requests pertaining to personal data transferred to third countries not covered by an adequacy decision

578. As explained in paragraphs 538 to 540, third-country legislation may lawfully[972] prohibit the controller from being informed of the request for disclosure of personal data processed in a third country where such legislation respects the essence of the fundamental rights and freedoms recognised by the Charter and must not exceed what is necessary and proportionate in a democratic society to safeguard one of the important objectives as also recognised in EU or Member State law, such as those listed in Article 25(1) of the Regulation.

579. Under the DPA, the law applicable to the requesting third party may prohibit Microsoft and its sub-processors from notifying the Commission of disclosure requests. The SCCs between Microsoft Ireland and Microsoft Corporation provide similarly that Microsoft Corporation may be prohibited from notifying Microsoft Ireland (which has an obligation to forward any such notification to the Commission) by the laws of the third country to which the data have been transferred.[973] It follows from paragraph 578 that the Commission must ensure that any prohibition of notification by Microsoft or by its sub-processors to the Commission of a request for disclosure of personal data, which they are processing on the Commission's behalf in a third country not covered by an adequacy decision, is based on third-country legislation that meets the condition recalled in that paragraph.

580. As demonstrated in paragraphs 377 to 414, on the reference date the Commission had not carried out a transfer impact assessment for transfers of personal data outside the EEA in the context of its use of Microsoft 365. Moreover, the Commission's transfer impact assessment carried out after the reference date did not assess the level of protection in all third countries to which transfers of personal data are envisaged under the 2021 ILA in the Commission's use of Microsoft 365. Nor did it properly assess the level of protection in the United States as regards transfers prior to the entry into force of the US adequacy decision. In doing so, the Commission has failed to assess whether the legislation of the third country to which personal data are envisaged to be transferred under the 2021 ILA and whose public authorities may make disclosure requests meets the condition referred to in paragraph 578. The Commission has therefore failed to ensure that any prohibition of notification in question meets the condition referred to in paragraph 578. This is in breach of Article 29(3)(a) of the Regulation, as interpreted in light of the *Schrems II* judgment.

---

[972] I.e. in compliance with the Regulation.

[973] Cf. Clause 14 of the processor to processor SCCs. See also https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/new-standard-contractual-clauses-questions-and-answers-overview_en#local-laws-and-governments-access, answer to question 41.

Disclosure requests pertaining to personal data transferred to third countries covered by an adequacy decision

581. The law of a third country covered by an adequacy decision is deemed to meet the condition referred to in paragraph 578. Such law may therefore lawfully[974] prohibit the notification to the Commission of a request by a public authority of that third country for disclosure of personal data processed in that third country.

582. However, a request for disclosure of such data may be made by a public authority of a third country not covered by an adequacy decision. In this scenario, the DPA provides that the law *applicable to the requesting third party* may prohibit Microsoft and its sub-processors from notifying the Commission of a request for disclosure. It follows that according to the DPA, Microsoft and its sub-processors may be prohibited by the law of a third-country not covered by an adequacy decision from informing the Commission of such a disclosure request even where the personal data concerned are processed in a third country covered by an adequacy decision.

583. As explained in paragraph 580, the Commission has failed to assess whether the legislation of the third country to which personal data are envisaged to be transferred under the 2021 ILA and whose public authorities may make disclosure requests meets the condition referred to in paragraph 578. Such public authorities may also make requests for disclosure of personal data processed in a third country covered by an adequacy decision. The Commission has therefore failed to ensure that any prohibition of notification in question meets the condition referred to in paragraph 578. This is in breach of Article 29(3)(a) of the Regulation, as interpreted in light of the *Schrems II* judgment.

Findings

584. It follows from all the foregoing that:

- by failing to provide in the contract that any prohibition of notification to the Commission of disclosure requests for personal data processed in the EEA is based exclusively on EU or Member State law to which Microsoft or its (sub-)processor is subject, and

- by failing to ensure that any prohibition of notification of disclosure requests for personal data processed outside of the EEA constitutes a necessary and proportionate limitation in a democratic society to safeguard one of the important objectives as also recognised in EU or Member State law, such as those listed in Article 25(1) of the Regulation, respecting the essence of the fundamental rights and freedoms recognised by the Charter,

the Commission has not complied with the requirement that the processor is only allowed not to inform the controller of the legal requirement to process data without the controller's documented instructions, where EU or Member State law, or third-country law that ensures a level of protection essentially equivalent to that in the EEA, to which the processor is subject, prohibits such information on important grounds of public interest. The Commission has therefore infringed Article 29(3)(a) of the Regulation, in particular as interpreted in light of the *Schrems II* judgment.

[974] I.e. in compliance with the Regulation.

585. To conclude, the Commission has failed to ensure, on the reference date and continuously thereafter until the date of issuing this decision, that it is notified of requests for disclosure of personal data processed by Microsoft or its sub-processors on its behalf within and outside of the EEA, as required by Article 29(3)(a) of the Regulation, in particular as interpreted in light of the *Schrems II* judgment.

Protocol (No 7) on the Privileges and Immunities of the European Union

586. In the preliminary assessment, the EDPS assessed compliance by the Commission in its use of Microsoft 365 also in light of the Protocol on the Privileges and Immunities of the European Union (the 'Protocol'). Preliminarily, the EDPS found several infringements of the Protocol, and in particular Articles 1, 2 and 5, as regards unauthorised disclosures of personal data. In particular, the EDPS preliminarily found that the Commission failed to ensure that Microsoft and its sub-processors unconditionally notify the Commission, and redirect and challenge any requests for disclosure of personal data within and outside of the EEA.

587. In their replies to the preliminary assessment, the Commission and Microsoft Ireland have disputed the EDPS' preliminary findings, and in particular asserted that compliance with the Protocol does not fall within the EDPS' competence.

588. The EDPS has decided, after having thoroughly assessed all relevant legal and factual circumstances, not to pursue, in this decision, the assessment of compliance by the Commission with the Protocol. Nonetheless, the EDPS considers that the protections afforded by the Protocol extend to personal data contained in the archives of the EU in so far as such archives contain personal data. The high level of protection that Article 16 of the Treaty on the Functioning of the European Union ('TFEU') and Article 8 of the Charter afford to personal data include, whenever applicable, the protection afforded by the Protocol in so far as archives of the EU 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. In view of the foregoing, the EDPS recommends that the Commission consider the above-mentioned provisions of the Protocol.

3.3.3. Findings

589. In view of the foregoing, the EDPS finds that the Commission, on the reference date and continuously thereafter until the date of issuing this decision:

a) has infringed Article 29(3)(a) of the Regulation, in particular as interpreted in the light of the *Schrems II* judgment, by not ensuring that, for personal data processed in the EEA, only EU or Member State law prohibits notification to the Commission of a request for disclosure, and that, for personal data processed outside the EEA, any prohibition of such notification constitutes a necessary and proportionate measure in a democratic society respecting the essence of the fundamental rights and freedoms recognised by the Charter;

b) has infringed Articles 4(1)(f), 33(1) and (2) and 36 of the Regulation, by:

- not having assessed the legislation of all third countries to which personal data are envisaged to be transferred under the 2021 ILA and thereby

failing to ensure that Microsoft and its sub-processors do not make disclosures of personal data within and outside of the EEA that are not authorised under EU law;

- failing to implement effective technical and organisational measures that would ensure processing in accordance with the principle of integrity and confidentiality within the EEA and, as part of an essential equivalence of the level of protection, also outside of the EEA.

4. USE OF CORRECTIVE POWERS

590. Under Article 52(3) of the Regulation, the EDPS is responsible for monitoring and ensuring the application of the provisions of the Regulation and of any other Union act granting protections to natural persons whose data are processed by EU institutions and bodies. To that end, the EDPS exercises the powers granted in Article 58 of the Regulation, including corrective powers under Article 58(2).

591. The following measures are without prejudice to any other or further action the EDPS might undertake.

592. The EDPS has decided to take the following corrective measures in respect of the infringements detailed in sections 3.1.3, 3.2.3 and 3.3.3:

592.1. to order the Commission, under Article 58(2)(j) of the Regulation and with effect from 9 December 2024, to suspend all data flows resulting from its use of Microsoft 365 to Microsoft and to its affiliates and sub-processors, located in third countries not covered by an adequacy decision as referred to in Article 47(1) of the Regulation, and to demonstrate the effective implementation of such suspension (*infringements set out in paragraphs 509.a and b, first indent, and 589*);

592.2. to order the Commission, under Article 58(2)(e) of the Regulation, to bring the processing operations resulting from its use of Microsoft 365 into compliance, and to demonstrate such compliance, by 9 December 2024, by:

592.2.1. carrying out a transfer-mapping exercise identifying what personal data are transferred to which recipients in which third countries, for which purposes and subject to which safeguards, including any onward transfers (*infringements set out in paragraph 509.a and b, first indent*);

592.2.2. ensuring that all transfers to third countries take place solely to allow tasks within the competence of the controller to be carried out *(infringement set out in paragraph 509.d*);

592.2.3. ensuring, by way of contractual provisions concluded pursuant to Article 29(3) of the Regulation and of other organisational and technical measures, that:

a) all personal data are collected for explicit and specified purposes (*infringements set out in paragraph 217.a and b)*;

b) the types of personal data are sufficiently determined in relation to the purposes for which they are processed (*infringements set out in paragraph 217.a and b)*;

c) any processing by Microsoft or its affiliates or sub-processors is only carried out on the Commission's documented instructions, unless, for processing within the EEA, required by EU or Member State law, or, for processing outside of the EEA, third-country law that ensures a level of protection essentially equivalent to that in the EEA, to which Microsoft or its affiliates or sub-processors are subject (*infringements set out in paragraphs 217.b and c, 509.a and 589)*;

d) no personal data are further processed in a manner that is not compatible with the purposes for which the data are collected, in accordance with the criteria laid down in Article 6 of the Regulation (*infringement set out in paragraph 217.d)*;

e) any transmissions to Microsoft Ireland or its affiliates and sub-processors located in the EEA comply with Article 9 of the Regulation (*infringement set out in paragraph 217.e*);

f) for personal data processed in the EEA, only EU or Member State law prohibits notification to the Commission of a request for disclosure, and, for personal data processed outside the EEA, any prohibition of such notification constitutes a necessary and proportionate measure in a democratic society respecting the essence of the fundamental rights and freedoms recognised by the Charter, as required by Article 29(3)(a) of the Regulation, in particular as interpreted in light of the *Schrems II* judgment (*infringement set out in paragraph 589.a*);

g) no disclosures of personal data by Microsoft or its sub-processors take place, unless, for personal data processed within the EEA, the disclosure is required by EU or Member State law, or, for personal data processed outside of the EEA, the disclosure is required by third-country law that ensures a level of protection essentially equivalent to that in the EEA, to which Microsoft or its affiliates or sub-processors are subject (*infringements set out in paragraph 589.b*).

592.3. to issue a reprimand to the Commission under Article 58(2)(b) of the Regulation (*all infringements*).

593. The EDPS has taken into account that numerous key provisions of the Regulation have been infringed, including the principles of purpose limitation, accountability and integrity and confidentiality, and the serious nature of those infringements. Those infringements have affected various processing operations, and to a significant extent all processing which involves a large number of data subjects.[975] Moreover, the

[975] Affected data subjects include not only all Commission's staff, but also staff of other EU institutions or bodies and other individuals, which e.g. cooperate with the Commission using the Commission's tools

infringements concern significant large-scale transfers which occur on an on-going basis[976] and cover processing of personal data that may enable tracking of user activities in extreme detail.[977] The infringements have also continued after the reference date. The EDPS considers these to be aggravating factors. The EDPS underlines that the continuation of infringements after the reference date is considered an aggravating factor because during this period the processing has not been brought into compliance.

594. As noted in the introduction of this decision, the current proceedings have a precedent. In 2019 and 2020, the EDPS carried out an investigation into the use of Microsoft products and services by EU institutions under the 2018 ILA. In March 2020, the EDPS issued its findings and recommendations to assist EU institutions in bringing those processing activities into compliance.[978] The EDPS found a number of concerning areas of non-compliance, such as non-compliant data processing agreement, insufficient purpose limitation, lack of control over location of data processing and what was transferred out of the EEA and how, as well as a lack of proper safeguards to protect data that left the EEA and risk of unlawful disclosure of data. The EDPS made a set of 37 recommendations to the EU institutions to assist them to address the identified non-compliance.[979] Notwithstanding the improvements that the Commission has made as referred to in paragraph 6, the investigation underlying the present decision has shown that as regards several of the most substantial concerns the Commission has made no significant progress since the conclusion of the EDPS' previous investigation to ensure compliance with EU law. The EDPS considers this to be an aggravating factor as well. In its reply to the preliminary assessment, the Commission rejects this aggravating factor, mainly because it considers that it had "*addressed practically all recommendations issued by the EDPS*".[980] The EDPS does not concur with this assessment. The present decision details numerous infringements of the Regulation that have not been remedied.

595. The EDPS considers the suspension of data flows to third countries not covered by an adequacy decision resulting from the Commission's use of Microsoft 365 (paragraph 592.1) an appropriate, necessary and proportionate corrective measure to remedy the infringements set out in paragraphs 509 and 589. Any decision to the contrary would gravely impinge on the rights of data subjects guaranteed by the Charter and the

based on Microsoft 365 or whose personal data are otherwise processed when the Commission carries out its tasks using Microsoft 365.

976 See para. 429 of this decision.

977 See para. 77 of this decision.

978 Annexed to EDPS letter of 23 March 2020 to all EU institutions and bodies. See EDPS Public Paper on Outcome of own-initiative investigation into EU institutions' use of Microsoft products and services.

979 The EDPS e.g. recommended to EU institutions (and bodies) that they should renegotiate their licence agreement and put in place contractual terms to clarify amongst others how to protect data being transferred. The EDPS made clear that – unless its recommendations were implemented - the contract with Microsoft should require that any processing of any personal data entrusted to Microsoft or its sub-processors by EU institutions (or bodies) should as a rule take place within the EU or the EEA. The EDPS also recommended that EU institutions (and bodies) should consider carefully any purchases of Microsoft products and services or new uses of existing products and services until after they have analysed and implemented the EDPS' recommendations. Where EU institutions (or bodies) planned to use Microsoft products and services they did not already use (such as Microsoft Office 365 or Microsoft Azure cloud services), they should perform comprehensive assessments of the data protection risks posed by those products and services prior to deploying them. The EDPS also emphasised to the EU institutions (and bodies) that the EU institutions (and bodies) had few guarantees under their contract with Microsoft 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.

980 Commission's reply of 25 May 2023, para 185.

Regulation. As clarified by the *Schrems II* judgment, where the EU institution or body as the controller fails to carry out a transfer impact assessment and thus fails to ensure an essentially equivalent level of protection for the personal data concerned, the supervisory authority is empowered (and indeed required by the *Schrems II* judgment[981]) to ensure that such transfers do not take place, e.g. by suspending the data flows. In particular, this applies where the controller is not able to take adequate (effective) supplementary measures to guarantee such protection,[982] as in the present case. This includes not being able to take effective technical and organisational measures required by the Regulation that would prevent unauthorised disclosures, in particular in case of requests for disclosure by public authorities of third countries not covered by an adequacy decision.

596. In its reply to the preliminary assessment, Microsoft Ireland argues that the EDPS should have carried out its own assessment of the level of protection in the third countries to which personal data are (envisaged to be) transferred under the 2021 ILA in order to satisfy its burden of proof before imposing a suspension of data flows.[983] In addition, Microsoft Ireland argues that the EDPS should have taken into account in its assessment the changes to the "*EU benchmark*" since the *Schrems II* judgment.[984] In this regard, the EDPS refers to paragraphs 396 to 411 of this decision.

597. The EDPS has taken note of the arguments put forward by the Commission[985] and Microsoft Ireland[986] with regard to the proportionality of the suspension of data flows. In order to ensure that the suspension of data flows does not compromise the ability of the Commission to carry out its tasks in the public interest or to exercise official authority, and to allow adequate time to implement the suspension, the EDPS has decided to delay the effect of this measure until 9 December 2024. The EDPS, however, notes that for an EU institution or body to carry out its tasks, it is not necessary to rely on Microsoft 365 cloud-based services (as opposed to Microsoft on-premise software),[987] even in a "*hybrid work environment of the post-pandemic situation*",[988] as demonstrated by the EDPS itself as well as numerous other EU institutions and bodies.[989]

---

[981] *Schrems II* judgment, paras. 105, 113, 121, 134 and 135. In this regard, the Court of Justice has, e.g., stated, by referring to point 148 of the opinion of Advocate General Saugmandsgaard Øe, that "*the supervisory authority is required, under Article 58(2)(f) and (j) of [the GDPR], to suspend or prohibit a transfer of personal data to a third country if, in its view, in the light of all the circumstances of that transfer, the standard data protection clauses* ***are not or cannot be complied with in that third country*** *and the protection of the data transferred that is required by EU law* ***cannot be ensured by other means****, where the controller or a processor has not itself suspended or put an end to the transfer*" (emphasis added).

[982] *Schrems II* judgment, paras. 133 and 135.

[983] See para. 391 of this decision.

[984] See paras. 392 and 393 of this decision.

[985] Commission's reply of 25 May 2023, in particular para. 175, and its arguments made at the hearing of 23 October 2023.

[986] Reply by Microsoft Ireland of 26 May 2023, in particular paras. 329 to 338, and its arguments made at the hearing of 23 October 2023.

[987] See, in this respect, EDPS Guidelines on the use of cloud computing services and EDPS Guidelines on the protection of personal data in IT governance and IT management of EU institutions.

[988] Commission's reply of 25 May 2023, para. 175.

[989] The EDPS does not consider the size and number of tasks that the Commission has to carry out to be a decisive distinguishing factor in this regard. Moreover, the EDPS rejects the argument put forward by Microsoft Ireland in its reply of 26 May 2023 (para. 359) that for cloud-based services, security updates are available immediately, whereas for software this may take longer, exposing the customer to security vulnerabilities. The EDPS stresses that in so far as the Commission remains adequately vigilant so as to apply any updates as soon as they are issued (and verified), as required by Articles 4(1)(f) and 33 of the

598. The EDPS considers that the imposed suspension of data flows does not constitute an excessive inconvenience or superfluous costs, as it is imperative to safeguard the rights and freedoms of data subjects. In particular, the Commission in its 2021 DPIA in which it documented its transfer impact assessment only focused on the United States, which is now covered by an adequacy decision.[990] This suggests that the Commission was and remains[991] convinced, that, despite indications to the contrary set out in this decision,[992] no transfers, including onward transfers, take place to (other) third countries not covered by an adequacy decision to which transfers are permitted and envisaged under the 2021 ILA.[993] The foregoing substantiates further that the suspension of data flows which is limited to third countries not covered by an adequacy decision is an entirely proportional corrective measure. Moreover, the EDPS notes that several infringements found affecting all processing in the Commission's use of Microsoft 365 may constitute grounds for the imposition of further limitations on processing.[994] However, the EDPS does not consider such measures proportionate at this time.

599. The corrective measures under paragraph 592.2 specify how the Commission is to bring the processing operations into compliance with the Regulation. As there are no other equally effective corrective measures available, they are appropriate, necessary and proportionate in relation to the infringements they seek to remedy. The evidence before the EDPS indicates that the processing cannot be brought into compliance with the Regulation without them. The corrective measures do not go beyond what is required by the Regulation. The order under paragraph 592.2 takes effect immediately. However, the corrective measures that it contains must be fully complied with by 9 December 2024. The EDPS considers this to be an appropriate and proportionate time to comply with the measures listed in paragraph 592.2.

600. The EDPS considers the corrective measures under paragraphs 592.2.3.f and g to be necessary for the Commission to ensure that no disclosures of personal data processed within or outside of the EEA take place to third-country authorities unless they are authorised under EU or Member State law, or third-country law that is essentially equivalent to that in the EEA.[995]

601. The EDPS considers that the infringements found could not have been remedied with an order to the Commission to use its rights under the 2021 ILA to audit Microsoft, as suggested by the Commission,[996] nor with an invitation to the Commission to renegotiate the 2021 ILA, as suggested by Microsoft Ireland.[997] In addition to the gravity and duration of infringements which warrant the measures imposed, an audit is in principle a tool of establishing facts regarding compliance, as also acknowledged by the

Regulation, the time delay compared to the updates applied to cloud-based services would be insignificant.

990 See para. 384 of this decision.

991 Given that the EDPS has received no information from the Commission as regards a further transfer impact assessment that would include the assessment of the laws and practices of other third countries not covered by an adequacy decision.

992 See e.g. paras. 338, 339, 384 and 385 of this decision.

993 2021 ILA, pp. 89 to 177.

994 In accordance with Article 58(2)(g) or (j) of the Regulation, the EDPS also has the corrective powers:
(g) "*to impose a temporary or definitive limitation including a ban on processing*";
(j) "*to order the suspension of data flows to a recipient in a Member State, a third country or to an international organisation*".

995 See also paras. 553, 555, 556, 584 and 585 of this decision.

996 Commission's reply of 25 May 2023, para. 181.

997 Reply by Microsoft Ireland of 26 May 2023, paras. 45 and 147.

Commission,[998] and not as a direct means of enforcement which is in this instance necessary to safeguard the rights and freedoms of data subjects. "*Inviting*" the controller to bring the processing in compliance is not one of the corrective measures envisaged under Article 58(2) of the Regulation, nor would a mere recommendation, without using corrective powers, be a sufficiently effective measure to remedy the infringements in view of all circumstances of this case. The EDPS has therefore decided to order the Commission to bring the processing into compliance, in a specific manner, as warranted by the infringements found.

602. The EDPS considers that in view of all infringements also a reprimand is an appropriate and necessary corrective measure (paragraph 592.3). A primary purpose of the EDPS' power to issue a reprimand under Article 58(2)(b) of the Regulation is to achieve a dissuasive effect and to make it clear to the EU institution concerned that it has infringed the Regulation.

603. Moreover, it is incumbent upon the Commission is to demonstrate compliance with the orders under paragraphs 592.1 and 592.2 by 9 December 2024. In doing so, the Commission also has to also provide its views and a description of the measures taken within the meaning of Article 59 of the Regulation in view of the order under paragraph 592.3. The EDPS notes that any failure by the Commission to comply with the orders under paragraphs 592.1 and 592.2 may result in the imposition of administrative fines in accordance with Article 66 of the Regulation. In such a case, the EDPS may make use of additional corrective powers provided for in Article 58(2) of the Regulation.

604. Pursuant to Article 64 of the Regulation, an action against this decision may be brought before the Court of Justice, within two months of its notification, in accordance with the conditions laid down in Article 263 TFEU.

Done at Brussels, 8 March 2024

[e-signed]

Wojciech Rafał WIEWIÓROWSKI

[998] Commission's reply of 25 May 2023, para. 181. The Commission suggests a measure ordering an audit "*in order to clarify factual aspects that the EDPS considers necessary*".

DETAILED TABLE OF CONTENTS