7

Opinion of the Board (Art. 64)

Opinion 22/2024 on certain obligations following from the reliance on processor(s) and sub-processor(s)

Adopted on 7 October 2024

Executive summary

The Danish SA requested the EDPB to issue an opinion on matters of general application pursuant to Article 64(2) GDPR. The opinion contributes to a harmonised interpretation by the national supervisory authorities of certain aspects of Article 28 GDPR, where appropriate in conjunction with Chapter V GDPR. In particular, the opinion addresses questions on the interpretation of certain duties of controllers relying on processors and sub-processors, arising in particular from Article 28 GDPR, as well as the wording of controller-processor contracts. The questions address processing of personal data in the EEA as well processing following a transfer to a third country.

The Board concludes in this opinion that controllers should have the information on the identity (i.e. name, address, contact person) of all processors, sub-processors etc. readily available at all times so that they can best fulfil their obligations under Article 28 GDPR, regardless of the risk associated with the processing activity. To this end, the processor should proactively provide to the controller all this information and should keep them up to date at all times.

Article 28(1) GDPR provides that controllers have the obligation to engage processors providing 'sufficient guarantees' to implement 'appropriate' measures in such a manner that the processing will meet the requirements of the GDPR and ensure the protection of the rights of data subjects. The EDPB considers, in its opinion, that when assessing compliance of controllers with this obligation and with the accountability principle (Article 24(1) GDPR), SAs should consider that the engagement of processors should not lower the level of protection for the rights of data subjects. The controller's *obligation* to verify whether the (sub-)processors present 'sufficient guarantees' to implement the appropriate measures determined by the controller should apply regardless of the risk to the rights and freedoms of data subjects. However, the *extent* of such verification will in practice vary depending on the nature of these technical and organisational measures, which may be stricter or more extensive depending on the level of such risk.

The EDPB further specifies in the opinion that while the initial processor should ensure that it proposes sub-processors providing sufficient guarantees, the ultimate decision on whether to engage a specific sub-processor and the pertaining responsibility, including with respect to verifying the guarantees, remains with the controller. SAs should assess whether the controller is able to demonstrate that the verification of the sufficiency of the guarantees provided by its (sub-)processors has taken place to the controller's satisfaction. The controller may choose to rely on the information received from its processor and build on it if needed (for example, where it seems incomplete, inaccurate or raises questions). More specifically, for processing presenting a high risk to the rights and freedoms of data subjects, the controller should increase its level of verification in terms of checking the information provided. In that regard, the EDPB considers that under the GDPR the controller does not have a duty to systematically ask for the sub-processing contracts to check whether the data protection obligations provided for in the initial contract have been passed down the processing chain. The controller should assess, on a case-by-case basis, whether requesting a copy of such contracts or reviewing them at any time is necessary for it to be able to demonstrate compliance in light of the principle of accountability.

Where transfers of personal data outside of the EEA take place between two (sub-)processors, in accordance with the controller's instructions, the controller is still subject to the duties stemming from

Article 28(1) GDPR on 'sufficient guarantees', besides the ones under Article 44 to ensure that the level of protection guaranteed by the GDPR is not undermined by transfers of personal data. The processor/exporter should prepare the relevant documentation, in line with the case-law and as explained in EDPB Recommendations 01/2020. The controller should assess and be able to show to the competent SA such documentation. The controller may rely on the documentation or information received from the processor/exporter and if necessary build on it. The extent and nature of the controller's duty to assess this documentation may depend on the ground used for the transfer and whether the transfer constitutes an initial or onward transfer.

The EDPB also addressed, in the opinion, a question on the wording of controller-processor contracts. In this respect, a basic element is the commitment for the processor to process personal data only on documented instructions from the controller, unless the processor is "*required to [process] by Union or Member State law to which the processor is subject*" (Article 28(3)(a) GDPR) - recalling the general principle that contracts cannot override the law. In light of the contractual freedom afforded to the parties to tailor their controller-processor contract to their circumstances, within the limits of Article 28(3) GDPR, the EDPB takes the view that including the words "*unless required to do so by Union or Member State law to which the processor is subject*" (either verbatim or in very similar terms) is highly recommended but not mandatory.

As to variants similar to "*unless required to do so by law or binding order of a governmental body*" the EDPB takes the view that this remains within prerogative of the contractual freedom of the parties and does not infringe Article 28(3)(a) GDPR per se. At the same time the EDPB identifies a number of issues in its opinion, as such a clause does not exonerate the processor from complying with its obligations under the GDPR.

For personal data transferred outside of the EEA, the EDPB considers it unlikely that the wording "*unless required to do so by law or binding order of a governmental body*", in itself, suffice to achieve compliance with Article 28(3)(a) GDPR in conjunction with Chapter V. As is illustrated by the European Commission's International Transfer SCCs and the BCR-C recommendations, Article 28(3)(a) GDPR does not prevent - on principle - the inclusion in the contract of provisions that address third country law requirements to process transferred personal data. However, as is the case in these documents, a distinction should be made between the third country law(s) which would undermine the level of protection guaranteed by the GDPR and those that would not. Finally, the EDPB recalls that the possibility of third country law impeding compliance with the GDPR should be a factor considered by the parties before entering into the contract (between controller and processor or between processor and sub-processor).

Where the processor is processing personal data within the EEA, it may still be faced with third country law, in certain circumstances. The EDPB underlines that the addition in the contract of wording similar to "*unless required to do so by law or binding order of a governmental body*" does not release the processor from its obligations under the GDPR.

Finally, the EDPB is of the opinion that following up the commitment of the processor to only process on documented instructions with "*unless required to do so by law or binding order of a governmental body*" (either verbatim or in very similar terms) cannot be construed as a documented instruction by the controller.

Table of contents

The European Data Protection Board

Having regard to Article 63 and Article 64(2) of the Regulation 2016/679/EU 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 (hereinafter "GDPR"),

Having regard to the EEA Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018[1],

Having regard to Article 10 and Article 22 of its Rules of Procedure,

Whereas:

(1) The main role of the European Data Protection Board (hereafter the 'Board' or the 'EDPB') is to ensure the consistent application of the GDPR throughout the European Economic Area ('EEA'). Article 64(2) GDPR provides that any supervisory authority ('SA'), the Chair of the Board or the Commission may request that any matter of general application or producing effects in more than one EEA Member State be examined by the Board with a view to obtaining an opinion. The aim of this opinion is to examine a matter of general application or which produces effects in more than one EEA Member State.

(2) The opinion of the Board shall be adopted pursuant to Article 64(3) GDPR in conjunction with Article 10(2) of the EDPB Rules of Procedure within eight weeks from when the Chair and the competent supervisory authorities have decided that the file is complete. Upon decision of the Chair, this period may be extended by a further six weeks taking into account the complexity of the subject matter.

HAS ADOPTED THE FOLLOWING OPINION:

1 INTRODUCTION

1.1 Summary of facts

1. On 5 July 2024, the Danish Supervisory Authority (hereinafter, the 'DK SA') requested the European Data Protection Board (hereinafter, the "EDPB" or the "Board") to issue an opinion in relation to controllers' accountability obligations with respect to the chain of processing and the relationship between controllers and its (sub-)processors (hereinafter 'the request').

2. The DK SA declared the file complete on 8 July 2024. The Chair of the Board considered the file complete on 9 July 2024. On the same date, the file was broadcast by the EDPB Secretariat. The Chair,

[1] References to "Member States" made throughout this opinion should be understood as references to "EEA Member States". References to the "Union" made throughout this opinion should be understood as references to the "EEA".

considering the complexity of the matter, decided to extend the legal deadline in line with Article 64(3) GDPR and Article 10(4) of the Rules of Procedure.

3. The DK SA also refers, in its request, to the report adopted by the EDPB in January 2023 on the findings of its first coordinated enforcement action[2] within the Coordinated Enforcement Framework (CEF)[3]. This coordinated action focused on the use of cloud-based services by the public sector. In the EDPB report, the supervisory authorities taking part in the coordinated action identified eight challenges in particular in relation to public bodies' use of cloud services and provided a list of points of attention for the relevant stakeholders to take into account when assessing cloud services and engaging with cloud services providers[4]. While for most of these points the extent of the obligations imposed by the GDPR is clear for both controllers and processors, the precise extent of certain obligations under the GDPR remains unclear according to the DK SA[5].

The following questions were asked by the DK SA:

4. Question 1.1: Taking into account Articles 5(2) and 24(1) GDPR, where engaging a processor to carry out processing on behalf of the controller, in order to document compliance with *inter alia* Article 28(1) and Article 28(2) (including when presenting documentation to the SA upon inspection):

    a. Must the controller identify all of the processor's sub-processors, their sub-processors, etc. throughout the processing chain, or only identify the first line of sub-processors engaged by the processor?

    b. to what extent and in which level of detail must the controller verify and document:

        i. the sufficiency of the safeguards provided by processors, their sub-processors etc.,
        ii. the content of the contracts between the initial processor and the additional processors to ascertain whether the same obligations have been imposed on the additional processors pursuant to Article 28(4) GDPR, and
        iii. whether the processors, their sub-processors etc. meet the controller's requirements under Article 28(1)?

5. Question 1.2: In cases of transfers or onward transfers from a (sub-)processor to another (sub-) processor in accordance with the controller's instructions: To what extent must the controller as part of its obligation under Article 28(1) GDPR, in conjunction with Article 44 GDPR, assess and be able to show documentation from (sub-)processors that the level of protection for personal data is not undermined by the (onward) transfers?

6. Question 1.3: Does the extent of the obligations under Articles 28(1) and 28(2) GDPR read in conjunction with Articles 5(2) and 24 GDPR, as answered in question 1.1 and question 1.2, vary depending on the risk associated with the processing activity? If so, what is the extent of such obligations for low-risk processing activities, and what is the extent for high-risk processing activities?

7. Question 2: Must a contract or other legal act under Union or Member State law pursuant to Article 28(3) GDPR contain the exception provided for in Article 28(3)(a) "*unless required to do so by Union or*

[2] Report on 2022 Coordinated Enforcement Action - Use of cloud-based services by the public sector, 17 January 2023 (hereinafter, "CEF Report on Cloud Services").
[3] The Coordinated Enforcement Framework was set up by the EDPB in October 2020 with a view to streamlining enforcement and cooperation among supervisory authorities. See EDPB Document on Coordinated Enforcement Framework under Regulation 2016/679, adopted on 20 October 2020, version 1.1.
[4] CEF Report on Cloud Services, p. 10-20.
[5] Request, p. 1.

Member State law to which the processor is subject" (either verbatim or in very similar terms) in order to be in compliance with the GDPR?

8. Question 2a: if the answer to question 2 is no, where a contract or other legal act under Union or Member State law that broadens the exception of Article 28(3)(a) GDPR to cover also third country law in general (e.g. "unless required to do so by law or binding order of a governmental body") is this in itself an infringement of Article 28(3)(a) GDPR?

9. Question 2b: If the answer to question 2a is no, should such a broadened exception instead be interpreted as a documented instruction by the controller in the sense of Article 28(3)(a) GDPR?

1.2 Admissibility of the request for an Article 64(2) GDPR Opinion

10. Article 64(2) of the GDPR provides that, in particular, any supervisory authority may request that any matter of general application or producing effects in more than one Member State be examined by the Board with a view to obtaining an opinion.

11. The first questions referred by the DK SA relates to the controllers' accountability obligations under Article 28 GDPR (questions 1.1, 1.2 and 1.3), while the last one referred to the specific content of the controller-processor contract or legal act under Article 28(3)(a) GDPR (question 2).

12. The Board considers that these questions are connected to the interpretation of the GDPR, particularly with respect to the relationship between the controllers and its (sub-)processors and to the interpretation of Articles 5(2), 24, and 28 GDPR. The request is linked to, on the one hand, the controllers' accountability obligations and the level of documentation that the supervisory authorities should expect from any controllers engaging (sub-)processors to carry out processing activities on their behalf and, on the other hand, the content of the controller-processor contracts or legal acts. Therefore, this request concerns a "*matter of general application*" within the meaning of Article 64(2) GDPR.

13. Moreover, the Board considers that the request of the DK SA is reasoned in line with Article 10(3) of the EDPB Rules of Procedure, as the DK SA has provided arguments in favour of the need for a consistent interpretation of the questions addressed in the request.

14. According to Article 64(3) GDPR, the EDPB shall not issue an opinion if it has already issued an opinion on the matter[6]. The EDPB has not yet provided replies to the questions arising from the DK SA's request. Further, the available EDPB guidelines, including in particular EDPB Guidelines 07/2020 on the concepts of controller and processor[7] (hereinafter "EDPB Guidelines 07/2020"), provide some guidance on the extent of the controller's accountability obligations under Article 28 GDPR but the existing guidance does not fully address all the questions set out in the request[8]. More specifically, for instance, the guidance that is available regarding Article 28(3)(a) GDPR does not specifically address the question included in the DK SA's request as to whether the terms "*unless required to do so by Union or Member State law to which the processor is subject*" should be included in controller-processor contracts or legal acts.

[6] Art. 64(3) GDPR and Art. 10(4) of the EDPB Rules of Procedure.
[7] EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR, version 2.1, Adopted on 07 July 2021.
[8] See in particular EDPB Guidelines 07/2020, Section 1.1 "Choice of the processor" on page 30, Section 1.3.4 "*The processor must respect the conditions referred to in Article 28(2) and 28(4) for engaging another processor (Art. 28(3)(d) GDPR)"* on page 37, Section 1.6 "Sub-processors", on page 42.

15. For these reasons, the Board considers that the DK SA's request is admissible and the questions arising from the DK SA's request should be analysed in an opinion adopted pursuant to Article 64(2) GDPR.

2 ON THE MERITS OF THE REQUESTERROR! BOOKMARK NOT DEFINED.

2.1 On the interpretation of Articles 28(1), 28(2) and 28(4) GDPR combined with Article 5(2) and Article 24(1) (questions 1.1 and 1.3)

16. This section addresses questions 1.1 and 1.3 referred to the Board, as reproduced in the 'admissibility' section above.

17. Article 28 GDPR sets out the relationship between the controller and the processor and imposes direct obligations on controllers and processors. As a preliminary remark, it should be noted that the GDPR defines "processor" in Article 4(8) in a general manner which includes both the initial processor engaged directly by the controller as well as the processor's processor, and so on along the processing chain.

18. The EDPB underlines that the assessment of the role of the parties (and whether they act as sole or joint controllers or as processors) falls outside of the scope of the request. The EDPB recalls that it is primarily up to the parties to assess their actual role depending on factual elements or circumstances of the case[9] without prejudice to the competence of the SA to check whether their assessment holds true.

19. In light of the questions above, this Opinion focusses solely on the scope and extent of the controller's obligations under Article 28(1) GDPR to verify whether the (sub-)processors provide "sufficient guarantees", under Article 28(2), and the controller's relating accountability obligations under Articles 5(2) and 24(1) GDPR[10].

20. In addition, the Board notes that the above questions do not relate to the controller's liability towards data subjects for the processing activities carried out on its behalf, for example with respect to data subjects' right to compensation under Article 82 GDPR. This section will therefore focus on providing clarifications to the SAs regarding the interpretation of Articles 28(1) and 28(2) GDPR combined with Article 5(2) and Article 24 GDPR on certain obligations following from the reliance on processor(s) and sub-processors. For the purpose of replying to these questions, the Board will conduct an analysis focusing on situations where there is no transfer of personal data outside of the EEA. In contrast, the section below on question 1.2 assesses situations where there are transfers taking place along the processing chain.

2.1.1 Identification of the actors in the processing chain

21. Concerning the question of whether, in essence, the controller should identify all of the processor's sub-processors, their sub-processors, etc. throughout the processing chain, or only identify the first

[9] EDPB Guidelines 07/2020, para. 12.

[10] This question is distinct and separate from any other obligations on the controller (or (sub-)processors) to ensure compliance with GDPR, e.g. with the principle of lawfulness, with Art. 32 or Chapter V GDPR obligations. The controller may still be responsible for processing under his controllership that is not in compliance with such GDPR provisions, even if he has met the obligations to verify his (sub-)processors in accordance with Art. 28(1) GDPR detailed in this Opinion, and this Opinion does not address the controller's responsibility for compliance with GDPR provisions other than Art. 24(1), 28(1) and 28(2) GDPR.

line of sub-processors engaged by the processor, the EDPB recalls, first of all, that "*Although the chain [of processing] may be quite long, the controller retains its pivotal role in determining the purpose and means of processing*"[11].

22. The EDPB reads the terms "identify" and "information on the identity" for the purposes of replying to the question as referring to the name, address, contact person (name, position, contact details) of the processor and the description of the processing (including a clear delimitation of responsibilities in case several sub-processors are authorised)[12].

23. With respect to the choice of processors, controllers should be in a position that allows them to effectively determine the purposes and means of the processing as per Article 4.7 GDPR. In that regards, determining the recipients (including processors) is considered an "essential means" of the processing, on which the controller decides[13].

24. To this end, with respect to the engagement of **additional processors** by the initial processor, the prior specific or general written authorisation of the controller is necessary under Article 28(2) GDPR. EDPB Guidelines 07/2020 clarified that the obligations foreseen by Article 28(2) are "*triggered when a (sub)processor intends to engage another player, thereby adding another link to the chain, by entrusting to it activities requiring the processing of personal data*"[14].

25. In cases where the controller decides to accept certain sub-processors at the time of the signature of the contract, a list of approved sub-processors should be included in the contract or an annex thereto. The list should then be kept up to date, in accordance with the general or specific authorisation given by the controller[15].

26. Concerning the engagement of sub-processors, the GDPR envisages the possibility for a general or specific authorisation. **In case of specific authorisation**, the controller should specify in writing which sub-processor is authorised and for what specific processing activity and time[16]. If the processor's request for a specific authorisation is not answered within the set timeframe, it should be interpreted as denied[17].

27. **In case of general authorisation**, the processor should give the controller the opportunity to approve a list of sub-processors at the time the general authorisation is signed and the opportunity - including

[11] EDPB Guidelines 07/2020, para. 152.

[12] This mirrors the information required for the identification of processors in Annex IV of the European Commission Controller-Processor SCCs (Commission implementing decision 2021/915 of 4 June 2021) and Annex III of the European Commission's international transfers SCCs (Commission implementing decision 2021/914 of 4 June 2021).

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

[14] EDPB Guidelines 07/2020, para. 151 reads: "*Data processing activities are often carried out by a great number of actors, and the chains of subcontracting are becoming increasingly complex. The GDPR introduces specific obligations that are triggered when a (sub-)processor intends to engage another player, thereby adding another link to the chain, by entrusting to it activities requiring the processing of personal data. The analysis of whether the service provider acts as a sub-processor should be carried out in line with what described above on the concept of processor*".

[15] EDPB Guidelines 07/2020, para. 154.

[16] EDPB Guidelines 07/2020, para. 153 & 155. Under Clause 7.7, option 1, of the EC Controller-Processor SCCs, the list of sub-processors specifically authorised by the controller should be found in Annex IV, which should be kept up to date.

[17] EDPB Guidelines 07/2020, para. 155.

a sufficient timeframe - to object to any subsequent changes in the sub-processors[18]. The Board recalls that it should be up to the initial **processor to proactively provide certain information** to the controller and "*the processor's duty to inform the controller of any change of sub-processors implies that the processor **actively** indicates or flags such changes toward the controller*"[19].

28. This means that the information relating to the identification of all of the processor's sub-processors should be easily accessible to the controller. The identification of those actors is particularly relevant for the controller to be able to have control over its processing activities for which it is responsible and may be held accountable in case of a violation of the GDPR.

29. The processor should therefore provide all information on how the processing activity will be carried out on behalf of the controller, including information on the sub-processor used[20] and a description of the processing that is entrusted to the sub-processor[21].

30. Other legal reasons justify the need for the controller to identify all processors and sub-processors Processors to whom data is disclosed or transferred are considered "recipients"[22].

- In order to comply with transparency requirements under Articles 13(1)(e) and 14(1)(e) GDPR, controllers should inform data subjects about the data recipients or categories of data recipients, being as specific and concrete as possible[23]. Information on the 'categories of recipients' has to also be included in the records of processing (Article 30(1)(d)).

- Article 15 GDPR provides for the right of access to, among others, information on the recipients or categories of recipients to whom the personal data have been or will be

[18] See also EDPB Guidelines 07/2020, para. 156: "*Alternatively, the controller may provide its general authorisation to the use of sub-processors (in the contract, including a list with such sub-processors in an annex thereto) (...)*". Also relevant in this context is EDPB Opinion 14/2019 on the draft Standard Contractual Clauses submitted by the DK SA (Art. 28(8) GDPR). Under Clause 7.7, option 2, of the European Commission Controller-Processor SCCs, the processor has the controller's general authorisation for the engagement of sub-processors from an agreed list and shall specifically inform in writing the controller of any intended changes of that list through the addition or replacement of sub-processors in advance.

[19] EDPB Guidelines 07/2020, para. 128 (emphasis added). See also footnote 14.

[20] EDPB Guidelines 7/2020, para. 143.

[21] See for example Annex IV of the EC Controller-Processor SCCs and Annex II of the EC international transfers SCCs

[22] Art. 4(9) GDPR ; WP29 Guidelines on transparency under Regulation 2016/679, adopted on 29 November 2017, as last Revised and Adopted on 11 April 2018, WP260 rev.01, endorsed by the EDPB (hereinafter, "WP29 Guidelines on transparency"), p. 37.

[23] WP29 Guidelines on transparency, p. 37 ("*In accordance with the principle of fairness, controllers must provide information on the recipients that is most meaningful for data subjects. In practice, this will generally be the named recipients, so that data subjects know exactly who has their personal data. If controllers opt to provide the categories of recipients, the information should be as specific as possible by indicating the type of recipient (i.e. by reference to the activities it carries out), the industry, sector and sub-sector and the location of the recipients*"); EDPB Guidelines 01/2022 on data subject rights - Right of access, Version 2.1, adopted on 28 March 2023, (hereinafter "EDPB Guidelines 01/2022 (right of access)"), para. 117 ("*already under Art. 13 and 14 GDPR information on the recipients or categories of recipients should be as concrete as possible in respect of the principles of transparency and fairness*"); see CJEU, judgment of 12 January 2023, *RW v Österreichische Post AG*, C-154/21, para. 25; AG opinion on CJEU C-154/21, para. 36 ("*Articles 13 and 14 of the GDPR [...] lay down an obligation on the part of the controller to provide the data subject with information relating to the categories of recipient or the specific recipients of the personal data concerning him or her where personal data are collected from the data subject and where personal data have not been obtained from the data subject*").

disclosed[24]. The Court of Justice clarified that this provision entails an obligation for the controller to provide the data subject with the actual identity of the recipients[25]. Outside of the type of cases, in which the controller may indicate to the data subject only the categories of recipients, in principle it should be always possible for the controller to retrieve the names of the recipients and provide the necessary information to the data subjects without undue delay.

- Article 19 GDPR provides that the controller shall communicate any rectification or erasure of personal data or restriction of processing to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. The CJEU clarified that the second sentence of Article 19 expressly confers on the data subject the right to be informed of the specific recipients[26].

31. While this is not explicit in these provisions, the Board considers that for the purpose of Article 28(1) and 28(2) GDPR, controllers should have the information on the identity of all processors, sub-processors etc. readily available at all times[27] so that they can best fulfil their obligations under the provisions mentioned above. Such availability is also necessary so that controllers can collect and assess all of the necessary information to meet the requirements under the GDPR, including so that they can reply to access requests under Article 15 GDPR without undue delay and reacting quickly to data breaches occurring along the processing chain. This would apply regardless of the risk associated with the processing activity.

32. To this end, the processor should proactively provide[28] to the controller all information on the identity of all processors, sub-processors etc. processing on behalf of the controller, and should keep this information regarding all engaged sub-processors up to date at all times. The controller and processor may include in the contract further details on how and in which format the processor is to provide this information, as the controller may want to request a specific format so that it is easier for the controller to retrieve it and organise it.

[24] Art. 15(1)(c) GDPR. EDPB Guidelines 01/2022 (right of access), para. 116-117.

[25] CJEU Judgment of 12 January 2023, *RW v Österreichische Post AG*,C-154/21, para. 51: "*Article 15(1)(c) of the GDPR must be interpreted as meaning that the data subject's right of access to personal data concerning him or her, provided for by that provision, entails, where those data have been or will be disclosed to recipients, an obligation on the part of the controller to provide the data subject with the actual identity of those recipients, unless it is impossible to identify those recipients or the controller demonstrates that the data subject's requests for access are manifestly unfounded or excessive within the meaning of Article 12(5) of the GDPR, in which cases the controller may indicate to the data subject only the categories of recipient in question*".
The Court acknowledged that the data subject may also "*elect merely to request information concerning the categories of recipient*". CJEU Judgment of 12 January 2023, *RW v Österreichische Post AG*, C-154/21, para. 43. EDPB Guidelines 01/2022 (right of access), para. 117.

[26] CJEU Judgment of 12 January 2023, *RW v Österreichische Post AG*,C-154/21, para. 41.

[27] This information is necessary for the controller to be able to fulfil their obligations also in case the sub-processing chain is broken because one (sub-)processor is unreachable, unwilling or insolvent and another (sub-)processor needs to be contacted.

[28] In order to comply with Art. 28(2) GDPR to enable the controller to decide on the addition of sub-processors as well to comply with Art. 28(1) GDPR to enable the controller to verify whether the (sub-)processors present sufficient guarantees to implement the technical and organisational measures.

2.1.2 Verification and documentation by the controller of the sufficiency of the guarantees provided by all the processors in the processing chain

33. The questions 1.1.b.i, 1.1.b.iii and 1.3 seek to provide clarifications as to which extent and in which level of detail the controller should verify and document the sufficiency of the safeguards provided by all the processors in the processing chain and to which extent the obligations under Articles 28(1) and 28(2) GDPR read in conjunction with Articles 5(2) and 24 GDPR vary depending on the risk associated with the processing activity. With respect to these questions, the Board underlines the following elements.

34. Article 5(2) GDPR enshrines the principle of accountability, by making the controller responsible for compliance with the data protection principles of Article 5(1) GDPR and for being able to demonstrate this compliance. Article 5(2) GDPR applies to all the general principles listed in Article 5(1) GDPR.

35. Article 24(1) GDPR includes the controller's obligation to demonstrate that processing is performed in accordance with the GDPR but further develops one of the duties on which the accountability principle applies: the implementation of 'appropriate technical and organisational measures'[29]. Article 24(1) GDPR refers to the notion of 'risk'[30] as being relevant to its application, as one of the criteria that the controller needs to take into account in assessing the appropriateness of such measures[31]. Article 24(1) GDPR also adds that these measures are to be reviewed and updated where necessary.

36. As stated by the CJEU, "*Article 5(2) and Article 24 of the GDPR impose general accountability and compliance requirements upon controllers of personal data. In particular, those provisions require*

[29] Judgment of 25 January 2024, *BL v MediaMarktSaturn Hagen-Iserlohn GmbH*, C-687/21, ECLI:EU:C:2024:72, para. 36: "*Article 24 of the GDPR lays down a general obligation, on the part of the controller of personal data, to implement appropriate technical and organisational measures to ensure that that processing is performed in accordance with that regulation and to be able to demonstrate this*".

[30] Recital 75 GDPR lists some examples of risks: "*processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage*"; Recital 76 specifies: "*The likelihood and severity of the risk to the rights and freedoms of the data subject should be determined by reference to the nature, scope, context and purposes of the processing. Risk should be evaluated on the basis of an objective assessment, by which it is established whether data processing operations involve a risk or a high risk*". As summarised by the CJEU "*according to recital 76 of that regulation, the likelihood and severity of the risk depend on the specific features of the processing in question and that risk should be subject to an objective assessment*." (CJEU, judgment of 14 December 2023, *Natsionalna agentsia za prihodite*, C-340/21, EU:C:2023:986, para. 36).

[31] As stated by the CJEU, "*Article 24(1) lists a number of criteria to be taken into account in assessing the appropriateness of such measures, namely, the nature, scope, context and purpose of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons*", judgment of 14 December 2023, *Natsionalna agentsia za prihodite*, C-340/21, EU:C:2023:986, para. 25. In the same ruling, the CJEU specified that "*The appropriateness of such measures must be assessed in a concrete manner, by assessing whether those measures were implemented by that controller taking into account the various criteria referred to (...) and the data protection needs specifically inherent in the processing concerned and the risks arising from the latter*", para. 30; also recalled in judgment of 25 January 2024, *BL v MediaMarktSaturn Hagen-Iserlohn GmbH*, C-687/21, ECLI:EU:C:2024:72, para. 38: "*It is apparent, accordingly, from the wording of Articles 24 and 32 of the GDPR that the appropriateness of the measures implemented by the controller must be assessed in a concrete manner, taking into account the various criteria referred to in those articles and the data protection needs specifically inherent in the processing concerned and the risks arising from the latter, and that all the more since that controller must be able to demonstrate that the measures it implemented comply with that regulation, a possibility which it would be deprived of if an irrebuttable presumption were accepted*". It must be noted that the CJEU analysis also pertains to Art. 32 GDPR.

controllers to take appropriate steps to prevent any infringements of the rules laid down in the GDPR in order to ensure the right to the protection of data" [32].

37. The accountability principle is addressed to the controller, including when the controller has entrusted processors or sub-processors with the processing of personal data on their behalf.

38. Pursuant to Article 28(1) GDPR, when a controller engages a processor to carry out processing of personal data on its behalf, the controller must only use a processor who can provide "*sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements*" of the GDPR "*and ensure the protection of the rights of the data subject*"[33]. As indicated in EDPB Guidelines 07/2020, the accountability principle is also reflected in Article 28 GDPR[34].

39. In this regard, the EDPB highlights that for the purpose of assessing compliance with Articles 24(1) and 28(1) GDPR SAs should consider that **the engagement of processors should not lower the level of protection for the rights of data subjects** compared to a situation where the processing is carried out directly by the controller. This refers to the engagement of the initial processor, but also to the engagement of additional processors along the processing chain, e.g. sub-processors and sub-sub-processors. Articles 24(1) and 28(1) GDPR should be interpreted as requiring the controller to ensure that the processing chain only consists of processors, sub-processors, sub-sub-processors (etc.) that provide 'sufficient guarantees to implement appropriate technical and organisational measures'. In addition the controller should be able to prove that it has taken all of the elements provided in the GDPR into serious consideration[35]. These considerations hold true even if the chain of processing can be long and complex with different processors, sub-processors, etc. involved at different stages of the processing activities. The controller should exercise due diligence in their selection of and oversight over their processors.

40. With respect to the choice of the **initial processor**, the controller should verify the sufficiency of the guarantees provided on a case-by-case basis taking into account the nature, scope, context and purposes of processing as well as the risks for the rights and freedoms of natural persons, on the basis of the type of processing entrusted to the processor[36]. Pursuant to Article 28(5) GDPR, adherence of a processor to an approved code of conduct under Article 40 GDPR or an approved certification mechanism under Article 42 GDPR may be used as an element by which to demonstrate sufficient guarantees.

41. As previously mentioned by the EDPB, the controller should take into account several elements when verifying the guarantees provided by processors[37], and an exchange of relevant documentation will often be required[38]. In any case, "[t]*he guarantees 'provided' by the processor are those that the processor is able to demonstrate to the satisfaction of the controller, as those are the only ones that*

[32] Judgment of 27 October 2022, *Proximus NV v Gegevensbeschermingsautoriteit*, C-129/21, ECLI:EU:C:2022:833, para. 81. Also see EDPB Guidelines 07/2020, para. 9.
[33] EDPB Guidelines 07/2020, para. 94.
[34] EDPB Guidelines 07/2020, para. 8.
[35] EDPB Guidelines 07/2020, para. 94.
[36] EDPB Guidelines 07/2020, para. 96.
[37] EDPB Guidelines 07/2020, para. 97-98 (referring to the processor's expert knowledge, reliability, and resources, as well as to the reputation of the processor on the market, and to the adherence to an approved code of conduct or certification mechanism).
[38] EDPB Guidelines 07/2020, para. 95 (where some examples are mentioned: privacy policy, terms of service, record of processing activities, records management policy, information security policy, reports of external data protection audits, recognised international certifications, like ISO 27000 series).

can effectively be taken into account by the controller when assessing compliance with its obligations"[39]. Neither Article 28(1) GDPR itself nor previous EDPB documents provide an exhaustive list of the documents or actions that the processor should show or demonstrate, as this largely depends on the specific circumstances of the processing[40]. For example, the controller may choose to draw a questionnaire as a means to gather information from its processor to verify the relevant guarantees, ask for the relevant documentation, rely on publicly-available information and/or certifications or audit reports from trustworthy third parties and/or perform on-site audits.

42. The EDPB has already specified that the obligation to use only processors 'providing sufficient guarantees' contained in Article 28(1) GDPR is a continuous obligation, and that the controller should, at appropriate intervals, verify the processor's guarantees[41].

43. In light of question 1.3 raised by the DK SA in its request regarding the risk associated with the processing, the EDPB emphasises that the notion of risk plays an important role in a number of provisions of the GDPR, in particular those relating to Chapter IV GDPR[42].

44. It is important to highlight that the reference to 'risk' in Article 24(1) and Recital 74 GDPR should not be interpreted as meaning that the controller can neglect or deviate from its obligations in the GDPR based on the mere fact that it considers the risk to data subjects' rights and freedoms as 'low'. The obligation to implement 'appropriate technical and organisational measures' to ensure compliance with the GDPR in line with Article 24(1) GDPR always applies, but the measures that are needed to achieve this result may vary depending on the risk[43].

45. While Article 28(1) GDPR does not make specific references to the 'risk', it implies the need to consider the level of the risk to the rights and freedoms of data subjects. The requirement in Article 28(1) to use only processors providing 'sufficient guarantees' to implement 'appropriate technical and organisational measures' should be interpreted as implying the need to consider the provision by the processors of sufficient guarantees to implement such measures in the light of the risks of the processing, as for instance the level of the security measures to be implemented also depends on the risks.

46. The risk associated with the processing activity plays an important role in determining the appropriateness of the technical and organisational measures, along with the other criteria cited in Article 24(1) GDPR**[44]**. Depending on the level of the risk associated with the processing activity (for example, if special categories of personal data are being processed), the controller may define stricter

[39] EDPB Guidelines 07/2020, para. 95.

[40] EDPB Guidelines 07/2020 para. 96 ("*The controller's assessment of whether the guarantees are sufficient is a form of risk assessment, which will greatly depend on the type of processing entrusted to the processor and needs to be made on a case-by-case basis, taking into account the nature, scope, context and purposes of processing as well as the risks for the rights and freedoms of natural persons. As a consequence, the EDPB cannot provide an exhaustive list of the documents or actions that the processor needs to show or demonstrate in any given scenario, as this largely depends on the specific circumstances of the processing*").

[41] EDPB Guidelines 07/2020, para. 99: "*including through audits and inspections where appropriate*".

[42] The term 'risk' is referred to in Art. 24, 25, 27, 30, 32, 33, 34, 35, 36 and 39 GDPR.

[43] CJEU, Judgment of 14 December 2023, *Natsionalna agentsia za prihodite*, C-340/21, EU:C:2023:986, para. 35: "*recital 74 of the GDPR highlights the importance of the controller being obliged to implement appropriate and effective measures and being able to demonstrate the compliance of processing activities with that regulation, including the effectiveness of the measures, which should take into account the criteria, associated with the characteristics of the processing concerned and with the risk presented by it, which are also set out in Articles 24 and 32 of that regulation*".

[44] Art. 24(1) refers to "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*".

or more extensive technical and organisational measures. Any processor should therefore provide sufficient guarantees to effectively implement the 'appropriate' measures defined by the controller.

47. The Board considers that **the controller's *obligation* to verify whether the (sub-)processors present sufficient guarantees to implement the measures determined by the controller should apply regardless of the risk to the rights and freedoms of data subjects.**

48. **However, the *extent* of such verification will in practice vary depending on the nature of these organisational and technical measures determined by the controller based on, among other criteria, the risk associated with the processing.** For example, where the processing activities present a lower risk to the rights and freedoms of data subjects, the corresponding 'appropriate measures' will be less strict. Therefore, the extent of the controller's verification may be less extensive in practice. Conversely, in the event of higher risks arising from the processing concerned, the controller's level of verification may be more important in terms of checking the sufficient guarantees presented by the entire processing chain, given that the 'appropriate measures' to implement are more extensive and robust to address the risks for data subjects.

49. In this regard, depending on the level of the risk associated with the processing activity, the controller may increase the level of its verification by verifying the sub-processing contracts by itself and/or also impose on the initial processor an extended verification and documentation.

50. In accordance with the accountability principle, any measure that is considered to be necessary to comply with the GDPR, also on the basis of the risk entailed by the processing, should be appropriately documented by the controller[45]. Such duty is facilitated by, on the one hand, the **assistance and audit obligations** imposed on the processors and, on the other hand, the **information provided by the initial processor** to the controller before the engagement of additional processors.

51. Firstly, the Board notes that processors have a duty to assist the controller in complying with certain GDPR requirements (under Articles 28(3)(e) and (f))[46]. More generally, the processor has a duty to make available to the controller all information necessary to demonstrate compliance with Article 28 (Article 28(3)(h))[47]. The controller should be fully informed as to the details of the processing that are relevant to demonstrate compliance with the obligations laid down in Article 28 GDPR, and the processor should provide all information on how the processing activity is carried out on behalf of the

[45] Regarding the burden of proof of the controller, see CJEU, judgment of 14 December 2023, *Natsionalna agentsia za prihodite*, C-340/21, EU:C:2023:986, para. 52 : "*It is clear from the wording of Article 5(2), Article 24(1) and Article 32(1) of the GDPR that the controller concerned bears the burden of proving that the personal data are processed in such a way as to ensure appropriate security of those data, within the meaning of Article 5(1)(f) and Article 32 of that regulation*"; also see CJEU Judgment of 25 January 2024, BL v MediaMarktSaturn Hagen-Iserlohn GmbH, C-687/21, ECLI:EU:C:2024:72, para. 42 "*in that regard, it must be pointed out that it follows from a reading of Articles 5, 24 and 32 of the GDPR together, read in the light of recital 74 thereof, that, in an action for compensation under Article 82 of that regulation, the controller concerned bears the burden of proving that the personal data are processed in such a way as to ensure appropriate security of those data, within the meaning of Article 5(1)(f) and of Article 32 of that regulation. Such an allocation of the burden of proof is capable not only of encouraging the controllers of those data of adopting the security measures required by the GDPR, but also in retaining the effectiveness of the right to compensation provided for in Article 82 of that regulation and upholding the intentions of the EU legislature referred to in recital 11 thereof*".

[46] See EDPB Guidelines 07/2020, para. 130-138.

[47] See EDPB Guidelines 07/2020, para. 143-145.

controller[48]. The contract should specify on how often and how this flow of information should take place[49].

52. Therefore, the controller may rely on the information provided by the processor, pursuant to Article 28(3)(h) GDPR, in complying with its duty of documentation of the measures adopted, provided that the information submitted by the processor actually demonstrates compliance. As the processor is well placed to know about the details of the processing it carries out and of the processing carried out by the sub-processors, it should proactively make available to the controller all relevant information[50].

53. The above also applies to sub-processors. Indeed processors are required to pass the assistance obligations down the processing chain (Article 28(4) GDPR).

54. Secondly, the **engagement of sub-processors**, as recalled above, is only possible with the controller's prior written authorisation, which could be specific or general. If the controller chooses to give its general authorisation, it "*should be supplemented with criteria to guide the processor's choice (e.g., guarantees in terms of technical and organisational measures, expert knowledge, reliability and resources)*"[51].

55. As explained by the EDPB, "[i]*n order to make the assessment and the decision whether to authorise subcontracting, a list of intended sub-processors (including per each: their locations, what they will be doing and proof of what safeguards have been implemented)) will have to be provided to the data controller by the processor*"[52]. This information is needed for the controller to comply with the accountability principle in Articles 5(2) and 24 and with provisions of Articles 28(1), 32, and Chapter V of the GDPR[53]. Regarding transfers of personal data outside of the EEA, the Board refers to the response provided below to question 1.2 asked by the DK SA.

56. As recalled by the EDPB, the initial processor should ensure that it proposes sub-processors providing sufficient guarantees[54]. The need for the initial processor to provide the above information shows that the **processor has a role to play in the choice of the sub-processors and in verifying the guarantees they provide, and should provide the controller with sufficient information**. This is also consistent with the fact that, regardless of the criteria indicated by the controller to choose additional processors, the initial processor remains fully liable to the controller for the performance of the sub-processors' obligations (Article 28(4) GDPR).

57. In this regard, even if, according to Article 28(4) GDPR, it is under the direct responsibility of the processor engaging a sub-processor to ensure that the same data protection obligations as set out in the initial contract between the controller and the processor are imposed on that other processor, this

[48] EDPB Guidelines 07/2020, para. 143.
[49] EDPB Guidelines 07/2020, para. 143.
[50] EDPB Guidelines 07/2020, para. 143, referring to Art. 28(3)(h): "*For instance, the relevant portions of the processor's records of processing activities may be shared with the controller. The processor should provide all information on how the processing activity will be carried out on behalf of the controller. Such information should include information on the functioning of the systems used, security measures, how the data retention requirements are met, data location, transfers of data, who has access to data and who are the recipients of data, sub-processors used, etc*.". The possibility for controller to carry out audit is also specified in para. 144: "*The goal of such audit is ensuring that the controller has all information concerning the processing activity performed on its behalf and the guarantees provided by the processor*."
[51] EDPB Guidelines 07/2020, para. 156.
[52] EDPB Guidelines 07/2020, para. 152.
[53] EDPB Guidelines 07/2020, footnote 69.
[54] EDPB Guidelines 07/2020, para. 159.

does not lift the responsibility of the controller to ensure compliance with the requirements of Article 28(1), and Article 24(1) GDPR and for being able to demonstrate this compliance.

58. **The ultimate decision on whether to engage a specific sub-(sub-)processor and the pertaining responsibility, including with respect to verifying the sufficiency of the guarantees provided by the (sub-)processor, remains with the controller**. As already recalled, in case of generic or specific authorisation, it is always up to the controller to decide whether to approve the engagement of this sub-processor or whether to object against it.

59. When assessing compliance with Articles 24(1) and 28(1) GDPR, SAs should assess whether the controller is able to demonstrate that the verification of the sufficiency of the guarantees provided by its sub-processors has taken place to the controller's satisfaction. This entails that the controller may choose to rely on the information received from its processor and if necessary build on it. For example, in case where the information received by the controller seems incomplete, inaccurate or raises questions, or where appropriate based on the circumstances of the case including the risk associated with the processing, the controller should ask for additional information and/or verify the information and complete/correct it if necessary.

60. More specifically, for processing presenting a high risk to the rights and freedoms of data subjects, the controller should increase its level of verification in terms of checking the information provided regarding the guarantees presented by the different processors in the processing chain.

2.1.3 Verification of the contract between the initial processor and the additional processorsError! Bookmark not defined.

61. The DK SA asks in essence whether and to what extent the controller has the duty to verify and document that the sub-processing contracts impose the same obligations on the additional processors.

62. Article 28(4)[55] imposes a direct obligation on processors in this regard. Moreover, Article 28(3)(d) requires the controller and processor to "stipulate" the obligation for the processor to respect the conditions referred to in Article 28(4) in their contract, thereby making this requirement a contractual obligation imposed on the processor. In other words, **the initial processor is legally and contractually required to pass down the same data protection obligations in the sub-processing contracts it concludes with additional processors**.

[55] Art. 28(4) GDPR: "*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*."

63. Similarly, the additional processors will be contractually required (by the initial processor) to impose the same data protection obligations on their own processors, and so on along the processing chain[56]. It is not required that the sub-processing contract is identical in wording to the data processing contract concluded with the initial processor[57].

64. The Board recalls that if a sub-processor fails to fulfil its obligations, the ultimate responsibility for the performance of that other sub-processor's obligations rests with the controller. However, the initial processor will remain liable to the controller so that the controller has the possibility to make a contractual claim against its initial processor if such processor fails to pass down the same data protection obligations in the sub-processing contracts.

65. Processors have a duty to make available to the controller all information necessary to demonstrate compliance with Article 28(3)(h) GDPR. Therefore, upon request of the controller, the initial processor will have to provide the sub-processing contracts between the initial processor and the additional processors.

66. In that regard, the European Commission's Controller-Processor Standard Contractual Clauses ('SCCs')[58] and International Transfer SCCs[59] provide the controller with the possibility to request a copy of the sub-processing contract between the initial processor and the additional processors. This possibility is also provided for by three Controller-Processor SCCs adopted by SAs[60]. This possibility is

[56] In EDPB - EDPS Joint Opinion 2/2021 on the European Commission's Implementing Decision on standard contractual clauses for the transfer of personal data to third countries, the EDPB and EDPS highlighted that the requirement of Art. 28(4) GDPR needed to be taken into account by the parties in a processor-to-processor relationship (para. 66).

[57] EDPB Guidelines 07/2020, para. 160: "*Imposing the "same" obligations should be construed in a functional rather than in a formal way: it is not necessary for the contract to include exactly the same words as those used in the contract between the controller and the processor, but it should ensure that the obligations in substance are the same*". The EDPB also notes that where two processors rely on Module Three (processor-to-processor) of the EC International Transfer SCCs, an additional warrantee is provided by the initial processor. Under Clause 8.1.d of the EC International Transfer SCCs the data exporter (the initial processor) warrants that it has imposed the same data protection obligations on the data importer (sub-processor) as set out in the contract or other legal act under Union or Member State law between the controller and the data exporter.

[58] Under Section 7 on the use of sub-processors, Art. 7(7)(c) of the EC Controller-Processor SCCs provides: "*At the controller's request, the processor shall provide a copy of such a sub-processor agreement and any subsequent amendments to the controller. To the extent necessary to protect business secret or other confidential information, including personal data, the processor may redact the text of the agreement prior to sharing the copy*". Commission implementing decision 2021/915 of 4 June 2021 on standard contractual clauses between controllers and processors under Article 28(7) of Regulation (EU) 2016/679 and Article 29(7) of Regulation (EU) 2018/1725 ('EC Controller-Processor SCCs').

[59] Module Two (controller-to-processor), Clause 9(c) of the EC International Transfer SCCs provides: "*The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy*". In addition, Module Three (processor-to-processor) provides that "*The data importer shall provide, at the data exporter's or controller's request, a copy of such a sub-processor agreement and any subsequent amendments. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy*". Commission implementing decision 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 ('EC International Transfer SCCs')

[60] DK SA Standard Contractual Clauses for the purposes of compliance with Art. 28 GDPR, in particular clause 7.5; LT SA Standard Contractual Clauses for the purposes of compliance with Art. 28 GDPR, in particular clause 18; SI SA Standard Contractual Clauses for the purposes of compliance with Art. 28 GDPR, in particular clause 6.5.

an expression of the controller's right of audit under Article 28(3)(h) GDPR. If requested by the controller, the processor should provide such a copy.

67. Nevertheless, the EDPB notes that the SCCs do not regulate whether a controller *must* request such a copy in order to comply with Article 28(1) GDPR.

68. In that vein, whether or not the controller chooses to request such a copy cannot determine the controller's responsibility. The processor also bears, in any case, legal and contractual obligations requiring it to impose the same data protection obligations as in the initial contract.

69. This said, the **controller does not have a duty to systematically ask for the sub-processing contracts to check whether the data protection obligations provided for in the initial contract have been passed down the processing chain**. The controller should assess, on a case-by-case basis, whether requesting a copy of such contracts or reviewing them at any time is necessary for it to be able to demonstrate compliance in light of the principle of accountability. In the context of exercising its right of audit under 28(3)(h), the controller should have a process in place to undertake audit campaigns in order to check by sampling verifications that the contracts with its sub-processors contain the necessary data protection obligations.

70. The need to request a copy of the sub-processing contract depends therefore on the circumstances of the case. For example, in case of doubts as to the processor's or sub-processor's compliance with the requirements of Articles 28(1) and 28(4) or upon request by the SA, the controller should ask for the contract for its review (e.g. in the event that the additional processor is affected by a data breach, or in case of other publicly available information or other information available to the controller), e.g. there may be templates of the sub-processor's data processing contract that do not meet the requirements of Article 28(3) GDPR.

71. To ensure compliance with Article 28(1) in light of the principle of accountability, a copy of the sub-processing contracts may help the controller demonstrate that its processors and sub-processors present sufficient guarantees, including that the processor complies with Article 28(4) GDPR.The EDPB observes that a controller may not be able to assess whether the guarantees provided in relation to a sub-processor are sufficient or not without having accessed and assessed the content of the sub-processing contract. While guarantees may be provided for in writing in the contract, contractual clauses cannot - by themselves - demonstrate that the sufficient guarantees are effectively implemented by the parties to the contract.

2.2 On the interpretation of Article 28(1) GDPR in conjunction with Article 44 GDPR (transfers in the processing chain - questions 1.2 and 1.3)

72. Question 1.2 of the request seeks to bring clarifications in cases of transfers or onward transfers from a (sub-)processor to another (sub-)processor, to what extent the controller should, as part of its obligation under Article 28(1) GDPR, in conjunction with Article 44 GDPR, assess the documentation from (sub-)processors that the level of protection for personal data is not undermined by the initial or onward transfers.

73. Question 1.3 seeks to bring clarifications about whether the extent of the obligations under Article 28(1) GDPR read in conjunction with Article 5(2) and Article 24 GDPR, as answered in question 1.2, varies depending on the risk associated with the processing activity. If so, the DK SA requested to know what the extent of such obligations for 'low-risk' and 'high-risk' processing activities is.

Introductory clarifications

74. For the sake of clarity, some introductory clarifications relating to those questions are provided in the context of this Opinion.

75. Firstly, the EDPB understands the term 'transfer' in the meaning set out in EDPB Guidelines 05/2021 on the interplay between Article 3 and Chapter V GDPR[61] (hereinafter "EDPB Guidelines 05/2021 (interplay)"), which also refer to EDPB Guidelines 3/2018 on the territorial scope of the GDPR[62]. As previously underlined by the EDPB, remote access from a third country constitutes a transfer if it fulfils the criteria set out in EDPB Guidelines 05/2021 (interplay)[63]. In any case, the existence of a transfer triggers the application of Chapter V GDPR.

76. Secondly, as question 1.2 refers to a situation where a (sub-)processor carries out an initial or onward transfer to another (sub-)processor, the controller is not the data exporter; rather, the data exporter is a processor, which transfers the personal data to another processor along the chain on behalf of the controller, and not to a separate controller. It excludes, therefore, personal data transferred to separate controllers including third-country tribunals, courts or administrative authorities. Therefore, the interpretation of Article 48 GDPR does not fall in the scope of these questions.

77. Thirdly, the EDPB notes that question 1.2 refers to transfers taking place along the processing chain in accordance with the controller's documented instructions under Article 28(3)(a) GDPR. It is worth highlighting that it is up to the controller to decide on whether a transfer of personal data outside of the EEA is possible as part of the processing activities entrusted to the (sub-)processors. The processor should refrain from carrying out any initial or onward transfer outside the instructions of the controller[64]. The controller's documented instructions with respect to initial or onward transfers of personal data are to be passed down along the processing chain[65].

78. Fourthly, the EDPB clarifies that the notion of risk referred to in question 1.3 should be understood as the risk to the rights and freedoms of the data subjects whose personal data are processed, within the meaning of Recitals 75 and 76 GDPR (as mentioned in paragraph 35 above).

The responsibility of the controller exists even if the (sub-)processors carry out the initial or onward transfers

79. When it comes to the substance of the Request, the EDPB already specified that "*(...) there will be a transfer situation where a processor (either under Article 3(1) or under Article 3(2) for a given processing (...)) sends data to another processor or even to a controller in a third country as instructed by its controller. In these cases, the processor acts as a data exporter on behalf of the controller and has to ensure that the provisions of Chapter V are complied with for the transfer at stake according to*

[61] 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 where para. 9 sets out the three cumulative criteria to qualify a processing operation as a transfer and more generally Section 2 details these criteria.

[62] EDPB Guidelines 05/2021 (interplay), para. 12 referring to EDPB Guidelines 3/2018 on the territorial scope of the GDPR, version 2.1, adopted on 12 November 2019 (with corrigendum dated 7 January 2020), page 5 and Sections 1–3. Please see in particular "d) Processor not established in the Union" under Section 2.

[63] EDPB Guidelines 05/2021 (interplay), para. 16.

[64] Art. 29 GDPR. As recalled by the EDPB, "*The contract should specify the requirements for transfers to third countries or international organisations, taking into account the provisions of Chapter V of the GDPR*" (EDPB Guidelines 07/2020, para. 119). For example, the controller may choose to prohibit transfers or to allow them only to specific countries.

[65] Art. 28(4) GDPR.

the instructions of the controller, including that an appropriate transfer tool is used. Considering that the transfer is a processing activity carried out on behalf of the controller, ***the controller is also responsible and could be liable under Chapter V, and also has to ensure that the processor provides for sufficient guarantees under Article 28****."*[66]

80. In other words, in case of a transfer, even if not carried out directly by the controller, but rather by a processor on behalf of the controller, the controller is still subject to duties coming from both Article 44 GDPR and Article 28(1) GDPR[67] [68].

The responsibility stemming from Article 44 GDPR

81. The obligations of Article 44 GDPR[69] are addressed to both processors (in the context of the Opinion, acting as data exporters) and controllers[70]. Processors and controllers should therefore both ensure that the level of protection of the personal data is not undermined by the initial or onward transfer, irrespective of the ground under which the transfer takes place[71]. For example, both the controller and the processor remain, in principle, responsible under Chapter V GDPR for an unlawful initial or onward transfer[72] and therefore could be both and individually be held liable in the event of an infringement.

The responsibility stemming from Article 28(1) GDPR

82. Under the accountability principle, controllers are required to take 'appropriate steps' to prevent any infringements of the rules laid down in the GDPR in order to ensure the right to the protection of data[73] and this includes preventing infringements of Chapter V GDPR. This responsibility applies before the transfer starts, and as long as the transferred personal data are processed in the third country.

83. As explained above in paragraphs 47-48, the *controller's obligation* to verify whether the (sub-)processors present sufficient guarantees to implement the measures determined by the controller under Article 28(1) GDPR[74] should apply regardless of the risk to the rights and freedoms of data subjects. However the *extent* of such verification will in practice vary depending on the nature of

[66] EDPB Guidelines 05/2021 (interplay), para. 19, emphasis added in bold.
[67] It is also relevant to indicate that Art. 28(1) GDPR refers to meeting the requirements of the GDPR, and thus, should be interpreted as including Chapter V provisions relating to initial or onward transfers of personal data to third countries. This covers both initial and onward transfers, see Art. 44 GDPR.
[68] For the purpose of this section of the Opinion, the duties stemming from Art. 44 and Art. 28(1) GDPR are addressed, it being specified that the controller is still subject to all obligations applicable to controllers under the GDPR.
[69] Art. 44 GDPR refers to the provisions of Chapter V GDPR.
[70] Art. 44 GDPR addresses both "the controller and processor" for compliance with Chapter V; also see Recital 101. For that reason, EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, version 2.0, adopted on 18 June 2021 ((hereinafter "EDPB Recommendations 01/2020") apply to "data exporters" (be they controllers or (sub-)processors processing personal data).
[71] CJEU judgment of 16 July 2020, *Data Protection Commissioner v Facebook Ireland Ltd, Maximillian Schrems* (hereinafter 'CJEU judgment Schrems II'), case C-311/18, ECLI:EU:C:2020:559, para. 92.
[72] The controller can claim back from its processor compensation corresponding to its part of responsibility, provided that the conditions set out under Art. 82(5) GDPR are fulfilled.
[73] Please see the section above on Art. 5(2) and 24(1) combined with Art. 28(1) GDPR.
[74] For the avoidance of a doubt, it should be clarified that the "appropriate technical and organisational measures" referred to in Art. 24(1) and 28(1) GDPR are not to be confused with the "supplementary measures", mentioned in EDPB Recommendations 01/2020 (para. 50:"'*Supplementary measures' are by definition supplementary to the safeguards the Article 46 GDPR transfer tool already provides and to any other applicable security requirements (e.g. technical security measures) established in the GDPR*", referring to Recital 109 of the GDPR and CJEU judgment Schrems II, para. 133).

the organisational and technical measures determined by the controller based on, among other criteria, the risk associated with the processing[75]. In that regard, the existence of an initial or onward transfer to third countries along the processing chain may increase the risks arising from the processing and therefore, has an impact on the 'appropriate' measures determined by the controller[76].

84. Upon request, the controller - assisted by the processor and sub-processors - should be able to demonstrate to the competent SA its compliance with the requirements of Article 28(1) GDPR. The appropriate documentation could be based - among others - on the information received from the processors in the context of the engagement of (sub-)processors[77] (see paragraphs 54-56), but also with the assistance of its processors, in accordance with Article 28(3)(h) GDPR (see paragraphs 51-52).

85. The controller also needs all relevant information to issue the required instructions to transfer the personal data to the respective third countries and to be able to comply with the accountability principle in Article 5(2) and Article 24 GDPR, and with provisions of Article 28(1), Article 32 and Chapter V GDPR[78]. The controller may object or not authorise the engagement of an additional processor where it would entail a transfer of personal data from the initial processor (as an exporter) to the envisaged additional processor (as an importer) on the basis of the information received.

86. In line with paragraph 58 above, the controller is ultimately responsible for any infringement of Article 28(1) GDPR when it comes to using (sub-)processors, and could be held liable for it. The EDPB highlights that practical difficulties invoked by controllers concerning control over the engagement of sub-processors by their processor – which may make it difficult for them to verify the 'sufficient guarantees', especially regarding transfers to third countries – do not exonerate the controller from its responsibilities in the processing[79].

87. Non-exhaustive examples of the documentation that the controller should assess and be able to show to the competent SA - transfer mapping, ground for transfer used, and where applicable, "transfer impact assessment" and supplementary measures - are described below.

The transfer mapping:

88. As a first step, where personal data will be transferred to third countries in connection with the use of (sub-)processors, the controller should assess and be able to show documentation relating to the transfer mapping[80]. The controller should ensure that a transfer mapping is carried out by the exporter (which processes personal data on its behalf), setting out which personal data are transferred

[75] Please see the definition of risk, as explained in paragraphs 35 and 78.

[76] Recital 116 GDPR provides: "*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*."

[77] Also see Clause 9(a) of Module Three (processor to processor) of the EC International Transfer SCCs and its Annex III; also see Clause 9(a) of Module Two (controller to processor); and Clause 7.7(a) of the EC Controller-Processor SCCs and its Annex IV "List of sub-processors". Both Annex II of the EC International Transfer SCCs and Annex IV of the EC Controller-Processor SCCs are to be completed with the following information on the sub-processors in case of a specific authorisation from the controller: name, address, contact person's name, position and contact details and a description of the processing. In addition, Annex I to the EC International transfer SCCs, Section B "Description of transfer" includes "For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing". Similarly, Annex II to the Controller-Processor SCCs includes "For processing by (sub-) processors, also specify subject matter, nature and duration of the processing".

[78] EDPB Guidelines 07/2020, para. 152, footnote 69.

[79] CEF Report on Cloud Services, p. 16.

[80] "Mapping" refers to the first step (so-called "Know your transfer") of EDPB Recommendations 01/2020, Section 2.1 "Step 1: Know your transfers". This first step applies regardless of the ground for the transfer.

(including remote access), where, and for which purposes[81]. The controller may rely on such mapping and if necessary build on it. For example, where the mapping received by the controller seems incomplete[82], inaccurate or raises questions, the controller should ask for additional information, verify the information and complete/correct it if needed.

89. The controller should receive this information[83] before an additional processor is engaged. It should also be recalled that the controller is subject to specific transparency requirements with regard to transfers to third countries under Articles 13(1)(f), 14(1)(f), 15(1)(c) and Article 15(2) GDPR and the requirement to maintain records of processing activities under Article 30(1)(d) and (e) GDPR. In order to meet these requirements, the controller should know where the sub-processors are located and where transfers – including remote access – take place[84].

The ground for transfer used, and where applicable, the "transfer impact assessment" and the supplementary measures:

90. The controller should assess and be able to show documentation relating to the ground for the transfer[85] on which the exporter relies in accordance with the controller's instructions[86]. This means that the controller should receive this information from the (sub-)processors/exporters before the transfers take place. The EDPB recalled in this context that the controller is subject to specific transparency requirements with respect to the "existence or absence of an adequacy decision" under Article 45 GDPR or "appropriate safeguards" provided in accordance with Article 46 GDPR (Articles 13(1)(f), 14(1)(f) and Article 15(2) GDPR[87]).

91. As regards the extent of the controller's duty to assess this documentation, it depends on the type of ground used for the initial or onward transfer by the (sub-)processors (as data exporter)[88]:

92. Transfers can be made on the basis of an **adequacy decision** if under Article 45 GDPR, the Commission has decided that a third country, territory or one or more specified sectors within that third country, or that an international organisation ensures an adequate level of protection. To assess whether the level of protection is adequate, the Commission takes into account – among other criteria – the rules for the onward transfer of personal data to another third country or international organisation which are complied with in that country or international organisation, case-law, as well as effective and enforceable data subject rights and effective administrative and judicial redress for the data subjects whose personal data are being transferred[89].

[81] It should be specified that the purposes are determined by the controller, along with the "essential means" of the processing (see EDPB Guidelines 07/2020, para. 40).
[82] E.g., if the mapping does not specify the sub-processors' location, or if transfers in the form of remote access are not mentioned in the mapping while they are taking place.
[83] As explained above in paragraphs 54-56.
[84] Such mapping is also necessary when the parties are completing the relevant annexes of the EC International Transfer SCCs and the EC Controller-Processor SCCs (please see footnote 80 above).
[85] EDPB Recommendations 01/2020, Section 2.2. "Step 2: Identify the transfer tools you are relying on".
[86] Art. 28(3)(a) GDPR.
[87] EDPB Guidelines 01/2022 (right of access), para. 122.
[88] In accordance with the controller's documented instructions with respect to transfers of personal data along the processing chain.
[89] See Art. 45 GDPR and WP29 Adequacy Referential, Adopted on 28 November 2017, WP 254, endorsed by the EDPB on 25 May 2018, page 7: "*Further transfers of the personal data by the initial recipient of the original data transfer should be permitted only where the further recipient (i.e. the recipient of the onward transfer) is also subject to rules (including contractual rules) affording an adequate level of protection and following the relevant*

93. Against this background, where a transfer is carried out by a (sub-)processor (on behalf of the controller) on the basis of an adequacy decision pursuant to Article 45 GDPR, the degree of verification required from the controller under Article 28(1) GDPR that its (sub-)processor presents sufficient guarantees as regards compliance with Chapter V GDPR should cover the following elements:

- whether the adequacy decision is in force[90],

- and whether the transfers carried out on behalf of the controller fall in the scope of such decision (e.g. in-scope categories of personal data or sectors)[91].

94. Where personal data transferred by a (sub-)processor (on behalf of the controller) on the basis of an adequacy decision are subject to an **onward transfer** from this third country, the level of protection of natural persons guaranteed by the GDPR for such onward transfer should also not be undermined[92]. In this regard, pursuant to Article 45(2)(a) GDPR, any adequacy decision issued by the European Commission covers, among others, the third countries' rules governing onward transfers. Hence, under Article 44 GDPR, the controller does not have to check these requirements on its own.

95. In terms of the controller's obligation under Article 28(1) GDPR, this means that the controller should ensure that the (sub-)processor provides 'sufficient guarantees' also with respect to onward transfers carried out by a (sub-)processor from an adequate country.

96. In the absence of an adequacy decision, transfers can be made subject to the provision of "**appropriate safeguards**" in accordance with **Article 46 GDPR**. In this case, the controller should assess the appropriate safeguards put in place and be attentive about any problematic legislation that could prevent the sub-processor from complying with the obligations established in its contract with the initial processor[93]. More specifically, the controller should ensure that such "a transfer impact assessment"[94] is carried out, in line with the case-law[95], and as explained in EDPB Recommendations 01/2020. The documentation relating to the appropriate safeguards put in place, the "transfer impact assessment" and the possible supplementary measures should be produced by the

instructions when processing data on the behalf of the data controller. The level of protection of natural persons whose data is transferred must not be undermined by the onward transfer. The initial recipient of the data transferred from the EU shall be liable to ensure that appropriate safeguards are provided for onward transfers of data in the absence of an adequacy decision. Such onward transfers of data should only take place for limited and specified purposes and as long as there is a legal ground for that processing".

[90] EDPB Recommendations 01/2020, para. 19: "*If you [the date exporter] transfer personal data to third countries, regions or sectors covered by a Commission adequacy decision (to the extent applicable), you do not need to take any further steps as described in these recommendations. However, you must still monitor if adequacy decisions relevant to your transfers are revoked or invalidated*."

[91] EDPB Recommendations 01/2020, para. 19.

[92] See Art. 44 GDPR: "*the conditions laid down in this Chapter are complied with (…), including for onward transfers from the third country or an international organisation to another third country or to another international organisation*".

[93] In that regard, see CJEU judgment Schrems II, paras. 132 and 133, where the contractual nature of the EC international Transfer SCCs is emphasised by the CJEU.

[94] This assessment is explained in further detail in EDPB Recommendations 01/2020, step 3 entitled "Assess whether the Article 46 GDPR transfer tool you are relying on is effective in light of all circumstances of the transfer".

[95] CJEU judgment Schrems II, para. 134.

processor/exporter[96] (where appropriate in collaboration with the processor/importer[97]). The controller can rely on the assessment prepared by the (sub-)processor and if necessary build on it. For example, where the assessment received by the controller seems incomplete, inaccurate or raises questions, the controller should ask for additional information, verify the information and complete/correct it if needed, keeping in mind that the assessment should be in line with EDPB Recommendations 01/2020 and the steps set out therein[98]. This includes identifying laws and practices relevant in light of all circumstances of the transfer[99] and identifying appropriate supplementary measures if necessary[100]. In this regard, the controller should pay particular attention whether the data exporter, i.e. the processor or sub-processor, has assessed whether there is anything in the law and/or practices in the third country that may impinge on the effectiveness of the appropriate safeguards of the ground for the transfer the exporter is relying on[101], particularly due to the legislation and practices governing access to the transferred personal data by the third country's public authorities[102].

97. Moreover and similarly to the transfers based on an adequacy decision (Article 45 GDPR, see above in paragraphs 94 and 95), where personal data are transferred by a (sub-)processor on the basis of appropriate safeguards under Article 46 GDPR, the controller's obligation under Article 28(1) GDPR also covers to satisfy itself that the (sub-)processor presents sufficient guarantees as regards **onward transfers**. Appropriate safeguards under Article 46 GDPR usually include provisions laying down rules that will govern any onward transfers[103]. This means that controllers do not have to verify whether those rules as such are in line with the requirements of Chapter V GDPR. However, controllers should be able to show documentation relating to such onward transfers. This means that the controller should receive this information from the (sub-)processors/exporters, showing that the importers actually comply with the requirements for onward transfers as laid down in the appropriate safeguards instrument.

2.3 On the interpretation of Article 28(3)(a) GDPR (question 2)

[96] EDPB Recommendations 1/2022 on the Application for Approval and on the elements and principles to be found in Controller Binding Corporate Rules (Art. 47 GDPR), adopted on 20 June 2023, version 2.1, para. 10: "(...) *it is, for instance, the responsibility of each data exporter to assess, for each transfer, on a case-by-case basis, whether there is a need to implement supplementary measures in order to provide for a level of protection essentially equivalent to the one provided by the GDPR*."

[97] In CJEU judgment Schrems II, para. 134, the CJEU noted that such verification exercise can be done in collaboration with the importer where appropriate. See also EDPB Recommendations 01/2020, Section 4.

[98] Please see in particular "Step 3: Assess whether the Article 46 GDPR transfer tool you are relying on is effective in light of all circumstances of the transfer", "Step 4: Adopt supplementary measures", and "Step 6: Re-evaluate at appropriate intervals", as explained in EDPB Recommendations 01/2020.

[99] CJEU judgment Schrems II, para. 126. See also EDPB Recommendations 01/2020, Section 2.3. "Step 3: Assess whether the Article 46 GDPR transfer tool you are relying on is effective in light of all circumstances of the transfer" and in particular para. 33. In CJEU judgment Schrems II, para. 134, the CJEU noted that such verification exercise can be done in collaboration with the importer where appropriate (also see EDPB Recommendations 01/2020, para. 30).

[100] Based on the case-law, it is for the controller or processor to verify, on a case-by-case basis and, where appropriate, in collaboration with the recipient of the data, whether the law of the third country of destination ensures adequate protection, under EU law, of personal data transferred pursuant to standard data protection clauses, by providing, where necessary, additional safeguards to those offered by those clauses (CJEU judgment Schrems II, para. 134). See also EDPB Recommendations 01/2020, Section 2.4., "Step 4: Adopt supplementary measures".

[101] See EDPB Recommendations 01/2020, Section 2.3 ("Step 3").

[102] See EDPB Recommendations 01/2020, para. 41 et seq.

[103] See e.g. Clause 8.7 (Module One), respectively 8.8 (Modules Two and Three) of the EC Transfer SCCs (Commission Implementing Decision 2021/914) of 4/6/2021.

98. To ensure a transparent allocation of responsibilities and liabilities both internally (between controllers and processors) and externally towards data subjects and regulators, under Article 28(3) GDPR, any processing of personal data by a processor must be governed by a contract or other legal act under EU or Member State law[104] between the controller and the processor. In accordance with Article 28(3)(a) GDPR, the contract shall stipulate, in particular, 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 Union or Member State law to which the processor is subject*". This provision also provides that "*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*".

99. The request refers to the existence of contracts that include a commitment to process personal data only upon instruction of the controller "*unless required to do so by law or binding order of a governmental body*" (omitting the reference to Union or Member State law). In this regard, several questions were referred to the EDPB, addressed together in the section below:

> 2 Must a contract or other legal act under Union or Member State law pursuant to Article 28(3) GDPR contain the exception provided for in Article 28(3)(a) "*unless required to do so by Union or Member State law to which the processor is subject*" (either verbatim or in very similar terms) in order to be in compliance with the GDPR?
>
> 2a If the answer to question 2 is no, where a contract or other legal act under Union or Member State law broadens the exception of Article 28(3)(a) GDPR to cover also third country law (e.g. "unless required to do so by law or binding order of a governmental body"), is this in itself an infringement of Article 28(3)(a) GDPR?

100. EDPB Guidelines 07/2020 recall "*the importance of carefully negotiating and drafting data processing agreements"* with regards to any EU or Member State legal requirement to which the processor is subject[105]. As to their contents, EDPB Guidelines 07/2020 note that a contract "*between the controller and processor must comply with the requirements of Article 28 GDPR in order to ensure that the processor processes personal data in compliance with the GDPR. Any such agreement should take into account the specific responsibilities of controllers and processors. Although Article 28 provides a list of points which must be addressed in any contract governing the relationship between controllers and processors it leaves room for negotiations between the parties to such contracts*"[106]. The room for negotiation is limited by the requirements set out in Article 28(3) GDPR.

[104] Hereafter, the term '**contract**' will be used to refer to 'a contract or other legal act under EU or Member State law'.
[105] EDPB Guidelines 07/2020, para. 121.
[106] EDPB Guidelines 07/2020, para. 109.

101. First of all, the commitment from the processor to only process personal data on documented instructions from the controller is a core element of the contract.

102. However, as acknowledged by Article 28(3)(a) GDPR, processors may lawfully process personal data - other than on documented instructions of the controller - in order to comply with legal obligations under EU or Member States laws (hereafter '**EU/MS legal requirement**'). The same provision also demands a commitment from the processor to inform the controller - in advance - where an EU/MS legal requirement to process / transfer personal data to a third country or an international organisation applies, unless that law prohibits such information on important grounds of public interest. This commitment is explicitly included with wording very similar to the one of Article 28(3)(a) GDPR in the EC Controller-Processor SCCs[107] and in several Standard Contractual Clauses, in particular the SCCs adopted by the Danish[108], Slovenian[109] and Lithuanian[110] SAs for the purposes of compliance with Article 28 GDPR.

103. Aside from a commitment to process only on documented instructions from the controller, Article 28(3)(a) GDPR thus contains three main elements: (a) a rule governing situations where a legal requirement obliges the processor to carry out processing of personal data that is not based on the controller's instructions, hence is not on the controller's behalf, (b) the need for the processor to inform the controller[111], and (c) the reference to such legal requirement as arising from EU or Member State law.

[107] See in particular Clauses 7.1(a) and 7.8(a):
- Clause 7.1.a: "*The processor shall process personal data only on documented instructions from the controller, unless required to do so by Union or Member State law to which the processor is subject. In this case, the processor shall inform the controller of that legal requirement before processing, unless the law prohibits this on important grounds of public interest. Subsequent instructions may also be given by the controller throughout the duration of the processing of personal data. These instructions shall always be documented*." (emphasis added). In their joint opinion on the draft EC SCCs, the EDPB and EDPS recommended to include the full wording of Art. 28(3)(a) (thus, adding a reference to the duty of the processor to inform the controller of the legal requirement) in order to enhance consistency. 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 Art. 28 (7) of Regulation (EU) 2016/679 and Art. 29(7) of Regulation (EU) 2018/1725, para. 38. The wording "*unless required to do so by Union or Member State law to which the processor is subject*" was already present in the draft SCCs.
- Clause 7.8.a: "*Any transfer of data to a third country or an international organisation by the processor shall be done only on the basis of documented instructions from the controller or in order to fulfil a specific requirement under Union or Member State law to which the processor is subject and shall take place in compliance with Chapter V of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725*." With regard to Clause 7.8(a), the EDPB and EDPS recommended the inclusion of a reference to the possibility for the processor to undertake transfers based on a specific requirement under Union or Member State law to which the processor is subject, which was not initially specified in the draft SCCs. Annex 2 to EDPB-EDPS Joint Opinion 1/2021, Comments to Clause 7.7(a).

[108] Danish SA Standard Contractual Clauses for the purposes of compliance with Art. 28 GDPR, in particular Clauses 4.1 and 8.2. In EDPB Opinion 14/2019 on the draft Standard Contractual Clauses submitted by the DK SA (Art. 28(8) GDPR), the EDPB recommended to include the wording of Art. 28(3)(a) in order to ensure legal certainty.

[109] Slovenian SA Standard Contractual Clauses for the purposes of compliance with Art. 28 GDPR, in particular clauses 3.1 and 7.2.

[110] Lithuanian SA Standard Contractual Clauses for the purposes of compliance with Art. 28 GDPR, in particular clauses 4.1, 22 and 23.

[111] Art. 28(3)(a) GDPR provides that where Union or Member State law requires the processor to process personal data, then "*the processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest*;".

104. In this context, the EDPB recalls that, as a general principle, contracts cannot override the law. This means that whether or not the clause provided for in Article 28(3)(a) GDPR ("*unless required to do so by Union or Member State law to which the processor is subject*") is included in a contract, it cannot prevent legal requirements from applying in addition to or, in some cases, in conflict with the contractual requirements. Further, in accordance with the general principle that a contract does not create obligations towards third parties, a contract cannot bind, for instance, the public authorities of a Member State or a third country[112].

105. All contracts between a controller and a processor need to address situations where the processor may be required by legislation to process personal data other than on the basis of the controller's instructions. Moreover, the processor's obligation to inform the controller before carrying out a processing that is not based on its instructions is also a core element of the contract, which needs also to be included [113].

106. For personal data processed outside of the EEA, the reference to EU or Member State law may not be very meaningful, given that a processor outside the EEA will only exceptionally be subject to EU or Member State legal requirements. In this respect, the EDPB notes that the EC International Transfer SCCs, which are intended to fulfil, in addition to the requirements of Article 46(1) and Article 46(2(d) GDPR, the requirements of Article 28(3) and (4) GDPR[114], do not contain a wording similar to the "unless" clause in Article 28(3)(a) GDPR. However the requirement to process personal data only on documented instructions from the controller unless required to do so by EU or Member State law is already addressed indirectly by clause 8.1 of the EC International Transfer SCCs.[115] In addition, this

[112] This is why the EC International Transfer SCCs include several safeguards requiring the exporter and the importer to assess the mandatory requirements of a third country's legislation before transferring the data to ensure that they do not go beyond what is necessary in a democratic society (Clause 14(a) to (d)), requiring the importer to notify the exporter in case of changes and the latter to act accordingly (Clause 14(e) and (f)), and imposing on the importer obligations in case of access by public authorities (Clause 15). See CJEU judgment Schrems II, para. 125 and 141.

[113] In EDPB Opinion 18/2021 on the draft Standard Contractual Clauses submitted by the Lithuanian SA (Art. 28 (8) GDPR), the EDPB recommended to include the last element of Art. 28(3)(a) in the SCCs (i.e. the obligation for the processor to inform the controller about the applicable legal requirement), EDPB Opinion 18/2021, para. 19.

[114] See recital 9 of the EC International Transfer SCCs "*Where the processing involves data transfers from controllers subject to Regulation (EU) 2016/679 to processors outside its territorial scope or from processors subject to Regulation (EU) 2016/679 to sub-processors outside its territorial scope, the standard contractual clauses set out in the Annex to this Decision should also allow to fulfil the requirements of Article 28(3) and (4) of Regulation (EU) 2016/679.*"

[115] Clause 8 on data protection safeguards (Module Two: Transfers from controller to processor) states in section 8.1 - instructions:
"*(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.*
(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions."
Similarly, in Module Three (Transfers from processor to processor) Clause 8 on data protection safeguards states in section 8.1 - instructions:
"*(a) The data exporter has informed the data importer that it acts as processor under the instructions of its controller(s), which the data exporter shall make available to the data importer prior to processing.*
(b) The data importer shall process the personal data only on documented instructions from the controller, as communicated to the data importer by the data exporter, and any additional documented instructions from the data exporter. Such additional instructions shall not conflict with the instructions from the controller. The controller or data exporter may give further documented instructions regarding the data processing throughout the duration of the contract.
(c) The data importer shall immediately inform the data exporter if it is unable to follow those instructions. Where the data importer is unable to follow the instructions from the controller, the data exporter shall immediately notify the controller."

does not mean the information obligation in Article 28(3)(a) GDPR is not addressed, considering the EC International Transfer SCCs explicitly include the need for the data importer to inform the data exporter if it is unable to follow the controller's instructions [116]. Consequently, the commitment from the processor to inform the controller where a legal requirement to process applies (whether stemming from EU or Member State law or third country law), follows from the EC International Transfer SCCs without using the exact wording "*unless required to do so by Union or Member State law to which the processor is subject*" of Article 28(3)(a) GDPR (element (c) mentioned above).

107. This is in line with the objective of Article 28(3)(a) GDPR to ensure that the controller is informed when the processor is required by law to process personal data other than upon the controller's instructions.

108. In light of the analysis above, the EDPB takes the view that including, in a contract between the controller and the processor[117], the exception provided for in Article 28(3)(a) GDPR "*unless required to do so by Union or Member State law to which the processor is subject*" (either verbatim or in very similar terms) is highly recommended, but not strictly required in order to be in compliance with Article 28(3)(a) GDPR. This position is without prejudice to the need for a contractual obligation to inform the controller when the processor is legally required to process personal data other than upon the controller's instructions, as envisaged by Article 28(3)(a) GDPR. Where it is clear that EU or Member State legal requirements are relevant to the processing, using the wording of Article 28(3)(a) GDPR would help to demonstrate compliance.

109. The EDPB now turns to whether a contract including a broader exception covering also third country law, such as for example an exception to the commitment to process the personal data only on documented instructions from the controller "*unless required to do so by law or binding order of a governmental body*", is in itself an infringement of Article 28(3)(a) GDPR.

110. This wording, if not accompanied by further specifications, can encompass two distinct situations which should be analysed separately in light of the legal context:

- the envisaged legal requirement or binding order follows from Union or (EEA) Member State law.
- the envisaged legal requirement or binding order follows from laws other than Union or (EEA) Member State law.

[116] In addition to Clause 8.1 (see previous footnote), Clause 14 states in section 14.e that: "*The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a). [For Module Three: The data exporter shall forward the notification to the controller.]*"

[117] In particular, where the controller and processor rely on their own processing contract, rather than on the EC Controller-Processor SCCs, on SCCs adopted by SAs for the purposes of compliance with Art. 28 GDPR or the EC International Transfer SCCs. See also recital 109 and 28(6) of Regulation (EU) 2016/679.

111. The first situation falls within the express provisions made by Article 28(3)(a) GDPR, setting out a contractual commitment for the processor to process only on documented instructions of the controller "*unless required to do so by Union or Member State law to which the processor is subject"*. This is the case regardless of whether the processing of personal data happens within or outside the EEA.

112. EU law, including the GDPR and Member State legal requirements are part of the same constitutional tradition as the GDPR, which enshrines the protection of natural persons in relation to the processing of personal data as a fundamental right., under Article 16(1) of the Treaty on the Functioning of the European Union (the '**TFEU**') and Article 8(1) of the Charter of Fundamental Rights of the European Union (the '**Charter**')[118].

113. Where the parties can demonstrate, based on other elements of their contract(s), that only this first situation is encompassed by the words "*unless required to do so by law or binding order of a governmental body"*, then this formulation does not have an impact on the guarantees provided by Article 28(3)(a) GDPR.

114. There will be cases where the parties' contract(s) go beyond this first situation, meaning that a reference to "*law or binding order of a governmental body*" encompasses legal requirements/binding orders arising from laws other than Union or (EEA) Member State law (second situation).

115. The EDPB notes that requirements to process data based on laws other than Union or (EEA) Member State law do not share the constitutional tradition per se, and cannot automatically be considered the same way as those within the EU legal order (in light of Article 44 GDPR). On this, the EDPB recalls that under Article 6 GDPR the terms 'legal obligation', 'public interest' and 'official authority' refer to Union or Member State law[119]. Likewise, the EDPB notes that Article 29 GDPR on processing under the authority of the controller or processor provides that "*[t]he 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*." (emphasis added)

116. In the context of transfers, it is foreseeable that legal requirements may arise also from legislation other than EU or Member State law. Where transfers are taking place, the EDPB recalls that Chapter V GDPR applies in addition to Article 28 GDPR. The EDPB takes the view that, with respect to personal data processed outside of the EEA, Article 28(3)(a) GDPR does not prevent - on principle - the inclusion, in the contract, of provisions that address third country law requirements to process transferred personal data. Such provisions may be included notably in order to ensure compliance with Chapter V

[118] Recital 1 GDPR refers to Art. 16(1) of the Treaty on the Functioning of the European Union (the 'TFEU') and Art. 8(1) of the Charter of Fundamental Rights of the European Union (the 'Charter'). Art. 52(1) of the Charter states that "*Any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others*."

[119] Art. 6(3) GDPR provides that where the legal basis for processing is 'legal obligation' (Art. 6(1)(c) GDPR) or 'a task carried out in the public interest or in the exercise of official authority vested in the controller' (Art. 6(1)(e) GDPR), this refers to provisions laid down in Union law or Member State law to which the controller is subject. In reference to Art. 6 GDPR, recital 40 GDPR explains that where the legal basis for processing is laid down by law, this means "*either in this Regulation or in other Union or Member State law as referred to in this Regulation*". Art. 49(4) GDPR provides that only public interests recognised in Union law or in the law of the Member State to which the controller is subject can lead to the application of this derogation.

GDPR, however merely including the words "*unless required to do so by law or binding order of a governmental body"* are highly unlikely to suffice.

117. In this context, the EDPB observes that the EC International Transfer SCCs specifically address 'Local laws and practices affecting compliance with the Clauses' in Clause 14 and 'Obligations of the data importer in case of access by public authorities' in Clause 15. Prior to signing SCCs, the parties must assess whether there are local laws and practices affecting compliance with the clauses (Clause 14 of the EC International Transfer SCCs). Clause 14 requires the parties to warrant that they are not aware of laws and practices in the third country where the importer is based that would prevent it from fulfilling its obligations under the EC International Transfer SCCs, following an assessment, by the importer, of such laws and practices, and requires the importer to promptly notify the exporter of any change, in which case either the exporter identifies appropriate measures to address the situation, or Clause 14 allows it to suspend the transfer and even to terminate the contract. Clause 15 imposes certain obligations on the data importer in case of access by third country public authorities. It lays down a number of steps the data importer must take when faced with third country government access (either upon request or directly), aiming to ensure (ultimately) that the controller is informed. Besides the obligation to notify the data exporter, the importer has inter alia the obligation to review the legality of the access request and document this legal assessment, and the duty to challenge the request in certain cases. The data exporter - in consultation with the controller where the data exporter is not the controller - will then be in a position to take the necessary measures, including possible suspension of the transfer or termination of the EC International Transfer SCCs. Whether any (onward) transfers to the third country government are compliant with the GDPR will depend on a case-by-case analysis (among other on the legal basis, controllership and compliance with Chapter V GDPR). Under module 3 of the EC International Transfer SCCs (Processor-to-Processor), the importer/processor has the obligation to make the legal assessment available to the exporter. In this respect, the EDPB also refers to paragraphs 88 - 89 and 106 above.

118. In addition, under the EC International Transfer SCCs, both the exporter and the importer are obliged to satisfy themselves that the legislation of the third country of destination enables the importer to comply with the EC International Transfer SCCs before transferring personal data to that third country[120]. Where the processor is exporting personal data on the controller's behalf, such obligation also falls on the controller (see also paragraphs 79 and following above).

119. Similarly, the BCR-controller recommendations and BCR-processor referentials also set out a set of obligations in the event that a BCR member is subject to a conflict between its local laws and the BCRs[121], and/or receives a request for disclosure from a law enforcement authority or state security

[120] CJEU judgment *Schrems II*, para. 141. See also EC International Transfer SCCs, Clause 14(a) to (d).

[121] Section 5.4.1 "Local laws and practices affecting compliance with the BCR-C", EDPB Recommendations 1/2022 on the Application for Approval and on the elements and principles to be found in Controller Binding Corporate Rules (Art. 47 GDPR). Section 6.3 "The need to be transparent where national legislation prevents the group from complying with the BCRs" of the Article 29 Working Party Working Document setting up a table with the elements and principles to be found in Processor Binding Corporate Rules, WP 257 rev.01, endorsed by the EDPB on 25 May 2018.

body[122]. More specifically, the EDPB Recommendations 1/2022[123] indicate that Binding Corporate Rules for Controllers (BCR-C) should contain clauses that address local laws and practices affecting compliance with the BCR-C (section 5.4.1) as well as obligations of the data importer in case of government access requests (section 5.4.2). BCR-C may serve as a transfer mechanism for transfers to processors within the group.

120. In cases where the transfers are covered by adequacy decisions, the legislation concerning "*access of public authorities to personal data as well as the implementation of such legislation*" is one of the elements the European Commission must take account of when assessing the adequacy of the level of protection, under Article 45(2)(a) GDPR[124].

121. What the adequacy decisions [125], the EC International Transfer SCCs [126] and the BCR recommendations and referentials [127] have in common is the understanding that laws and practices of a third country that respect the essence of the fundamental rights and freedoms enshrined in the TFEU, the Charter, and the GDPR and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) GDPR, will not undermine the level of protection ensured by the GDPR [128]. For this reason, the EC International Transfer SCCs [129] and the BCR recommendations and referentials [130] include provisions which attach different consequences to laws

[122] Section 5.4.2 "Obligations of the data importer in case of government access requests", EDPB Recommendations 1/2022 on the Application for Approval and on the elements and principles to be found in Controller Binding Corporate Rules (Art. 47 GDPR); see also Section 6.3 "The need to be transparent where national legislation prevents the group from complying with the BCRs", Working Document setting up a table with the elements and principles to be found in Processor Binding Corporate Rules, WP 257 rev.01.

[123] EDPB Recommendations 1/2022 on the Application for Approval and on the elements and principles to be found in Controller Binding Corporate Rules (Art. 47 GDPR).

[124] The CJEU addressed this element in its Schrems I and Schrems II rulings. CJEU judgment of 6 October 2015, *Maximillian Schrems v Data Protection Commissioner, (*hereinafter *'*CJEU judgment Schrems I**'**), case C-362/14, ECLI:EU:C:2015:650, para. 91 ff. CJEU judgment Schrems II, paras 141, 174-177, 187-189.

[125] See Art. 45(2)(a) GDPR which provides that the European Commission shall take into account "*the rule of law, respect for human rights and fundamental freedoms, relevant legislation, both general and sectoral, including concerning public security, defence, national security and criminal law and the access of public authorities to personal data, as well as the implementation of such legislation, data protection rules, professional rules and security measures, including rules for the onward transfer of personal data to another third country or international organisation which are complied with in that country or international organisation, case-law, as well as effective and enforceable data subject rights and effective administrative and judicial redress for the data subjects whose personal data are being transferred;*". See also Article 29 Working Party Adequacy Referential WP 254 rev.01, Adopted on 6 February 2018, endorsed by the EDPB on 25 May 2018. The concept of "adequate level of protection" has been further developed by the CJEU in its Schrems I (paragraphs 73 and 74) and Schrems II (para. 94) ruling.

[126] Clause 14.a of the EC International Transfer SCCs.

[127] This is explicit in the EDPB Recommendations 1/2022 (the BCR-C recommendations), version 2.1, under 5.4.1 and 5.4.2. The same understanding implicitly underpins section 6.3 "The need to be transparent where national legislation prevents the group from complying with the BCRs" of the Article 29 Working Party Working Document setting up a table with the elements and principles to be found in Processor Binding Corporate Rules, WP 257 rev.01, endorsed by the EDPB on 25 May 2018.

[128] EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, v. 2.0, para. 38, and EDPB Recommendations 02/2020 on the European Essential Guarantees for surveillance measures, paras. 22 and 24.

[129] Clause 14 of the EC International Transfer SCCs.

[130] See footnote 127.

and practices depending on whether they undermine the level of protection ensured by the GDPR. Ad hoc contracts based on Article 46(3)(a) GDPR should also contain similar provisions[131].

122. It is clear from the above that, when laws of the third country require the processor to process personal data other than upon the instructions of the controller, the level of protection enshrined in the GDPR will only be respected if said laws fulfil the abovementioned conditions. In any case, the processor should implement supplementary measures in case that said conditions are not met and the contract should ensure that these conditions are met.

123. When the processor is processing personal data within the EEA, it may still be faced with third country law, in certain circumstances. The EDPB underlines that the addition in the contract to a reference to third country law does not release the processor from its obligations under the GDPR.

124. In light of the analysis above, the EDPB takes the view that including wording similar to "*unless required to do so by law or binding order of a governmental body*" is a prerogative of the contractual freedom of the parties and does not infringe Article 28(3)(a) GDPR per se. This is without prejudice to the obligation to comply with the GDPR whenever personal data are processed. Moreover, such a clause does not exonerate the controller and processor from complying with their obligations under the GDPR, in particular regarding the information to be provided to the controller and - where applicable - the conditions for international transfers of the personal data processed on behalf of the controller.[132]

125. Last, the request asks a follow-up question:

> If the answer to question 2a is no, should such a broadened exception instead be interpreted as a documented instruction by the controller in the sense of Article 28(3)(a) GDPR?

126. In light of the reply given above, the EDPB understands the remaining question to be whether parties can claim the wording "*unless required to do so by law or binding order of a governmental body*" (either verbatim or in very similar terms) in their contract is to be construed as a documented instruction by the controller in the sense of Article 28(3)(a) GDPR.

127. The EDPB first considers whether this argument is tenable where the legal requirement or binding order follows from Union or (EEA) Member State law.

128. The EDPB notes that the notion of 'instructions' as used in Article 28(3)(a) GDPR pertains specifically to the controller setting out what data processing the processor is expected to do on their behalf and how[133]. Any provision that the controller includes in the contract with its service provider / processor that does not consist of a request to carry out processing of personal data on the controller's behalf also does not qualify as instruction in the sense of Article 28(3)(a) GDPR. Further, the controller's instructions would need to be sufficiently precise to cover a specific processing of personal data, which is not the case with the wording in question. Moreover, the controller would always (have to) be in a position – and legally required to the extent that an instruction to process personal data on the controller's behalf would be in breach of the GDPR – to withdraw such instruction. The processor should then comply with the controller's withdrawal of its instruction and discontinue the processing.

[131] EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, v. 2.0, para. 66.
[132] In particular, the controller's obligation to ensure that, with respect to processing outside the EEA, only third-country law that ensures an essentially equivalent level of protection may require processing by the processor. See also paragraphs 116 - 122 above.
[133] EDPB Guidelines 07/2020, para. 116.

129. By giving instructions to the processor, the controller puts in practice its determination of purposes and means of data processing, specifically by exerting influence over the key elements of the processing[134]. In principle, the controller's influence over personal data processing ceases where EU or Member State laws set out requirements for the processor to carry out processing of personal data that the controller is not in a position to steer or halt[135]. While the controller might remind the processor to abide by EU or Member State law, this cannot be understood as an instruction in the meaning of Article 28(3)(a) GDPR[136]. The GDPR itself acknowledges this state of affairs, precisely by pointing out that the processor must only process upon documented instruction of the controller, unless required to do so by Union or Member State law to which the processor is subject (Article 28(3)(a) GDPR), and must immediately inform the controller if an instruction infringes the GDPR (Article 28(3) GDPR last sub-paragraph).

130. The EDPB considers that the reasoning above applies also where the legal requirement or binding order follows from third country law. In this situation, the law in question limits the influence the controller can exert over the data processing.

131. In addition to the above, a clause whereby a processor commits to processing personal data only on documented instructions from the controller "*unless required to do so by law or binding order of a governmental body*" indicates in itself that processing upon instruction of the controller is the rule, whereas the exception exists precisely for processing not upon instruction of the controller (as shown by the word "unless"). Further, it is still the decision of the processor whether it complies with the legal request or binding order to which it is subject or whether it faces the legal consequences of not doing so.

132. On this basis, the EDPB concludes that "*unless required to do so by law or binding order of a governmental body*" (either verbatim or in very similar terms) cannot be construed as a documented instruction by the controller. The controller remains responsible where it has not ensured that the (sub-)processor processes personal data only on its documented instructions. However, this is not applicable where processing is required by EU or Member State law, or for processing outside the EEA, required by third-country law to which the (sub-)processor is subject and that law ensures an essentially equivalent level of protection.

For the European Data Protection Board

The Chair

(Anu Talus)

[134] EDPB Guidelines 07/2020, para. 20.

[135] In this regard, the situation could then be the one foreseen by Art. 4(7) GDPR, which states that where the purposes and means of processing are determined by Union or Member State law the controller or the specific criteria for its nomination may be provided by Union or Member State law. See CJEU judgment of 11 January 2024, *Belgian State (Données traitées par un journal officiel),* case C-231/22, ECLI:EU:C:2024:7, para. 28-30, 35 and 39; EDPB Guidelines 07/2020, para. 22-24.

[136] Rather, such a reminder will be considered as the controller putting in place contractual safeguards to ensure that the processing on the controller's behalf will comply with all the requirements of the GDPR and will ensure the protection of the rights of the data subject.