Opinion 7/2024 on the draft decision of the German North Rhine Westphalia Supervisory Authority regarding the EU Cloud Service Data Protection (Auditor) certification criteria

Adopted on 17 April 2024

Table of contents

The European Data Protection Board

Having regard to Article 63, Article 64(1)(c) and Article 42 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 European Economic Area (hereinafter "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 64(1)(c) GDPR and Articles 10 and 22 of its Rules of Procedure.

Whereas:

(1) Member States, supervisory authorities, the European Data Protection Board (hereinafter "the EDPB") and the European Commission shall encourage, in particular at Union level, the establishment of data protection certification mechanisms (hereinafter "certification mechanisms") and of data protection seals and marks, for the purpose of demonstrating compliance with the GDPR of processing operations by controllers and processors, taking into account the specific needs of micro, small and medium-sized enterprises[2]. In addition, the establishment of certifications can enhance transparency and allow data subjects to assess the level of data protection of relevant products and services[3].

(2) The certification criteria form an integral part of any certification mechanism. Consequently, the GDPR requires the approval of national certification criteria of a certification mechanism by the competent supervisory authority (Articles 42(5) and 43(2)(b) GDPR), or in the case of a European Data Protection Seal, by the EDPB (Articles 42(5) and 70(1)(o) GDPR.

(3) When a supervisory authority (hereinafter "SA") intends to approve a certification pursuant to Article 42(5) GDPR, the main role of the EDPB is to ensure the consistent application of the GDPR, through the consistency mechanism referred to in Articles 63, 64 and 65 GDPR. In this framework, according to Article 64(1)(c) GDPR, the EDPB is required to issue an Opinion on the SA's draft decision approving the certification criteria.

(4) This Opinion aims to ensure the consistent application of the GDPR, including by the SAs, controllers and processors in the light of the core elements which certification mechanisms have to develop. In particular, the EDPB assessment is carried out on the basis of "Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation" (hereinafter the "Guidelines") and their Addendum providing "Guidance on certification criteria assessment" (hereinafter the "Addendum"), for which the public consultation period expired on 26 May 2021.

[1] References to "Member States" made throughout this Opinion should be understood as references to "EEA Member States".
[2] Article 42(1) GDPR.
[3] Recital 100 GDPR.

(5) Accordingly, the EDPB acknowledges that each certification mechanism should be addressed individually and is without prejudice to the assessment of any other certification mechanism.
(6) Certification mechanisms should enable controllers and processors to demonstrate compliance with the GDPR; therefore, the certification criteria should properly reflect the requirements and principles concerning the protection of personal data laid down in the GDPR and contribute to its consistent application.
(7) At the same time, the certification criteria should take into account and, where appropriate, be inter-operable with other standards, such as ISO standards, and certification practices.
(8) As a result, certifications should add value to an organisation by helping to implement standardized and specified organisational and technical measures that demonstrably facilitate and enhance processing operation compliance, taking account of sector-specific requirements.
(9) The EDPB welcomes the efforts made by scheme owners to elaborate certification mechanisms, which are practical and potentially cost-effective tools to ensure greater consistency with the GDPR and foster the right to privacy and data protection of data subjects by increasing transparency.
(10) The EDPB recalls that certifications are voluntary accountability tools, and that the adherence to a certification mechanism does not reduce the responsibility of controllers or processors for compliance with the GDPR or prevent SAs from exercising their tasks and powers pursuant to the GDPR and the relevant national laws.
(11) The Opinion of the EDPB shall be adopted, pursuant to Article 64(1)(c) of GDPR in conjunction with Article 10(2) of the EDPB Rules of Procedure, within eight weeks from the first working day after the Chair and the competent SA 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.
(12) The EDPB Opinion focusses on the certification criteria. In case the EDPB requires high level information on the evaluation methods in order to be able to thoroughly assess the auditability of the draft certification criteria in the context of its Opinion thereof, the latter does not encompass any kind of approval of such evaluation methods.

HAS ADOPTED THE FOLLOWING OPINION:

1 SUMMARY OF THE FACTS

1. In accordance with Article 42(5) GDPR and the Guidelines, the Auditor certification criteria (hereinafter the "draft certification criteria" or "certification criteria") were drafted by EU Cloud Service Data Protection, a legal entity in Germany and submitted to the DE North Rhine Westphalia Supervisory Authority (hereinafter the "DE SA").

2. The DE SA has submitted its draft decision approving the certification criteria, and requested an Opinion of the EDPB pursuant to Article 64(1)(c) GDPR on 12 February 2024. The decision on the completeness of the file was taken on 15 February 2024. The Chair decided to extend the deadline for the adoption of this Opinion by further 6 weeks on 16 February 2024.

2 ASSESSMENT

3. The Board has conducted its assessment in line with the structure foreseen in Annex 2 to the Guidelines (hereinafter "Annex") and its Addendum. Where this Opinion remains silent on a specific section of the DE SA's draft certification criteria, it should be read as the Board not having any comments and not asking the DE SA to take further action.

4. These certification criteria are national criteria pursuant to Article 42(5) GDPR and are not intended to be an EU Data Protection Seal.

5. The present certification is not a certification according to article 46(2)(f) GDPR meant for international transfers of personal data and therefore does not provide appropriate safeguards within the framework of transfers of personal data to third countries or international organisations under the terms referred to in letter (f) of Article 46(2). Indeed, any transfer of personal data to a third country or to an international organisation, shall take place only if the provisions of Chapter V GDPR are respected.

2.1 GENERAL REMARKS

6. The Board takes note that although the certification is specifically targeting the data processing of cloud providers, the certification scheme defines general criteria applicable to data processors and also provides specific guidance related to the activity of cloud providers.

7. The Board notes that the certification criteria define three protection categories. Depending on the protection category selected by the cloud provider during the certification application process, the criteria used to evaluate the target of evaluation vary. Consequently, the cloud user remains responsible for selecting the appropriate certified cloud service based on its protection category, in order to demonstrate the "sufficient guarantees" of Article 28 GDPR.

8. The Board wishes to highlight the consequence of the following statement regarding the applicant as the controller of the data processing operation and the legal basis for data processing listed in criteria N° 13: *"As part of the AUDITOR certification, only those data processing operations are considered, which are performed by the cloud provider in order to provide the cloud service to the cloud user so as to enable the use of the service and invoice the user accordingly for the service."* The Board understands that if the cloud provider puts in place data processing operations that are not necessary to the performance of the contract with the cloud user when providing its service, its service is out of scope of the Auditor certification mechanism.

9. The Board notes that throughout the draft certification criteria, specific language corresponding to GDPR terminology or other concepts and definitions are used. As a general remark, the Board encourages the DE SA to ensure that when the GDPR terms are used in the certification criteria, they are in line with the GDPR as well as to include a statement in the beginning of the criteria, explaining that where the certification criteria use terms that are defined in the GDPR, those terms shall have the same meaning as in the GDPR. In particular:

    - section A. 1 refers to "auditor object of certification" which corresponds to the target of evaluation (ToE) and using the latter would enhance clarity;

- in section C, chapter 1, No 1.3 “Nature and purposes of data processing”, the draft certification criteria states that “The legally binding Commissioned Data Processing Agreement must determine the nature and purpose of the intended data processing in the order, the nature of data processed and the categories of data subjects”. In this regards, using the term “type” instead of “nature” of data processed would mirror the wording of Article 28(3) GDPR.

- in section C, chapter 1, No 1.8 “Return of data media and erasure of data; demonstrating compliance and allowing for and contribute to audits”, referring to the return of all personal data, as Article 28(3)(g) GDPR provides would ensure consistency.

- in section C, chapter 2, No 2.4 (4) “Access control”, the draft certification criteria state that “minimum level of protection must be provided to make intentional manipulation more difficult to achieve”. This lowers the guarantees provided by Article 32(1) GDPR and redrafting would be appropriate to ensure consistency with the GDPR, taking also into account the risk-based approach that the corresponding criterion already encompasses at its beginning, e.g. replace this sentence by “It shall be demonstrated that the TOMs ensure that intentional manipulation is prevented”.

- similarly, in section C, chapter 2, No 2.6 (2) “Traceability of data processing”, the draft criteria refer to the fact that “ the cloud provider must provide a minimum level of protection against intentional manipulation of the traceability measures, which makes such manipulation more difficult”. The Board is of the opinion that redrafting would be appropriate to be more consistent with the level of protection enshrined in the GDPR e.g., “It shall be demonstrated the TOMs ensure that intentional manipulation of the traceability measures is prevented”.

10. The board notes that criterion No 9.1 (1) refers to “conceptual objectives”. The Board recommends clarifying the meaning of this term.

11. The Board considers that the wording “inappropriate risks” (criteria 9.2 and 19.2) is unclear and should be further elaborated. Similarly, the term “inappropriate access” is used in criteria 2.4 which should refer to “unauthorized access” instead, in line with Article 32(2) GDPR. Thus, the Board recommends to further specify in the criteria what “inappropriate risks” entails and to refer to the appropriate GDPR terminology in criteria 2.4.

12. Furthermore, the Board notices that the draft certification criteria refer to the following terms:
    - Section A, 1 “content or application data”;
    - Section A, 1 “business”;
    - Section A, 1 “consumer”;
    - Section A, 1 “B2B”;
    - Section A, 1 “B2C”;
    - Section A, 1 “usage data”;
    - Section A, 1 “Commissioned Data Processing Agreement”.

    The Board welcomes the use of these terms. However, to enhance the readability and understanding of the certification criteria the Board recommends that the above-mentioned terms be clearly defined, taking also into account, where necessary, other areas of law (e.g. Directive 93/13/EEC of 5 April 1993). To this purpose, the Board encourages that either a new “terms and definitions” section is added or that relevant terms are clearly defined within the criteria.

13. Similarly, the criteria refer to the concept of "acts of god". It could be useful to refer to the concept of "force majeure" ("höhere Gewalt" in German) to ensure consistency with the European law acquis. This concept is used in numerous instruments and areas of European law and its definition was well settled in case-law by the CJEU on various occasions (See for example point 53 in Case C-640/15, ECLI:EU:C:2017:39). Therefore, the Board, in order to avoid any misunderstandings, encourages to refer to this EU law concept and to provide a definition accordingly[4].

14. Furthermore, the Board notes that in p. 7 the draft certification criteria refer to "personal data as goods to be protected". The Board is of the opinion that such term is not easily comprehensive nor legally sound. Therefore, the Board recommends the DE SA to replace this term with the term "information".

15. In addition, the Board takes note of section 2.5 on "transfer of data and transport encryption" and section 2.7. The Board understands that the term transfer refers to the transmission of the data and not to their transfer as per the GDPR meaning, particularly in Chapter V GDPR. Therefore and in order to avoid confusion, the Board encourages that the term "transfer" is replaced with the term "transmission".

16. In addition, the Board underlines that the criteria aim at defining a transparent level of data protection. Criteria requiring "a minimum level of protection" (criteria 2.2 (3) and 2.10 (2)), or "with sufficient certainty" (criterion 2.3 (8)), or "equally appropriate measures" (criteria 2.5 and 2.6 (6)), or "comply with the current technical recommendations (best practice)" (criterion 2.9(4)), fail to reach this objective and could lead to inconsistent assessment conducted by the certification bodies. Therefore, the EDPB recommends to modify the criteria listed above in order to ensure a clearer definition of the level of data protection.

2.2 SCOPE OF THE CERTIFICATION MECHANISM AND TARGET OF EVALUATION (TOE)

17. The Auditor certification scheme is only open to private sector cloud providers acting as processors for cloud users (being organisations or natural persons in the private sector) that are acting as controllers. Also data processing operations of the cloud provider acting as controller which are necessary to provide its cloud services to the cloud user may be certified under the scheme.

18. According to the scheme documentation, Auditor certification covers "*data processing operations that are provided in products or services, or with the assistance of products and services (including more than one)*". The scheme documentation further clarifies that the certification mechanism covers data processing operations that the cloud provider performs:

    (i) as a processor "*on behalf of a cloud user in accordance with Art. 28 GDPR*";

[4] "force majeure must be understood as referring to abnormal and unforeseeable circumstances which were outside the control of the party by whom it is pleaded and the consequences of which could not have been avoided in spite of the exercise of all due care"

(ii) as a controller "*in order to enter into and perform the contract with the cloud user for the provision of the cloud service"*; and

(iii) as a controller *"to fulfil legal obligations*".

With respect to point (ii) above, the Board considers that the scheme does not make it clear which processing operations would or would not be covered as being performed "*in order to enter into and perform the contract with the cloud user for the provision of the cloud service".* Thus, the Board recommends that the scope of the scheme be further specified to include:

(i) specified, explicit and legitimate categories of purposes of data processing operations where the cloud provider acts as controller; and

(ii) examples of processing operations that:

a. can be certified under the scheme; and

b. cannot be certified under the scheme.

This clarification is essential in order to identify the appropriate legal basis, pursuant to Article 6 GDPR and to ensure the respect of principles relating to the processing of personal data, pursuant to Article 5 GDPR.

19. The Board acknowledges that, where the cloud user is a natural person, some scenarios may arise where the GDPR would not apply to the processing of personal data by that natural person in the course of a purely personal or household activity (the so-called "household exemption" or "personal exemption", foreseen by Article 2(2)(c) GDPR). In such a scenario, the GDPR would still apply to the cloud provider acting as a processor and providing the means for such processing (as indicated by Recital 18 GDPR). However, not all use cases under a business-to-consumer relationship will entail the applicability of the household/personal exemption and the Board recommends to clarify in the criteria the situations in which the household/personal exemption would not apply to the cloud user who is a natural person.

20. The Board also highlights that the application of the personal/household exemption to the cloud user shall not affect the GDPR obligations that are applicable to the cloud service provider, when in such a scenario the latter is a processor. Particularly in this case, the cloud service provider shall comply with all the relevant obligations deriving from Article 28 GDPR. As such, the Board recommends that the scheme is amended to make it clear what adaptations are required to the certification criteria when the household/personal exemption is applicable vis-à-vis the cloud user (i.e. identify which criteria do not apply in this case or have specific criteria to cover this situation).

21. The Board notes that the criteria catalogue lacks specific provisions or considerations regarding the processing activities related to technical support and service maintenance of cloud services, especially if these activities entail access to personal data. The Board therefore encourages to clarify that the processing of personal data resulting from support or maintenance activities be explicitly addressed by the AUDITOR certification scheme, such that users have a clear understanding and assurance regarding how personal data is handled during these essential tasks.

22. For transparency reasons, the conditions to be met in order to establish the non-applicability of a criterion shall be an integral part of the criteria by default. The Board also acknowledges

that some criteria may not be relevant depending on the data processing circumstances. Such specificities need to be justified and documented so that the cloud user is informed about the reasons why some criteria could not be assessed. However, the Board recommends to further elaborate the following criteria when the conditions for the non-applicability are defined by the GDPR :

- the criteria 8.1 in order to define the conditions to be met to justify that a data protection officer was not designated ;

- the criteria 8.3 in order to define the conditions to be met to justify that records of processing activities are not maintained ;

- the criteria 16 in order to define the set of factors that need to be considered when assessing risk to the rights and freedoms of data subjects, as defined in the EDPB Guidelines 9/2022 on personal data breach notification under GDPR.

2.3 PROCESSING OPERATION, ARTICLE 42(1)

23. With regards to criteria 1.5, the EDPB encourages to clarify that the information required in criteria 1.5 (place of data processing) also includes the location of processing activities conducted by sub-processors when the applicant engages another processor for carrying out specific processing activities on behalf of the controller.

2.4 LAWFULNESS OF PROCESSING

24. The Board notes that the draft criterion 13 (1) attempts to reflect the requirements of Article 6(1)(b) GDPR by specifying that "*The cloud provider* [as controller] *may only process personal data and carry out processing operations that are necessary for the performance of a contract to which the cloud user is a party or for taking steps at the request of the cloud user prior to entering into a contract*". However, because "cloud user" is defined as a controller in the scheme, meaning the cloud user may be an organisation or a natural person, this criterion does not reflect the requirement of Article 6(1)(b) that a controller may only process personal data if necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract. Therefore, the Board recommends that the words "cloud user" in criteria 13 (1) are replaced by the words "data subject", and further amends the explanation part of the same criteria.

25. The Board notes that the draft criterion 13 (3) states that "*The cloud provider* [as controller] *may only process personal data and carry out processing operations that are necessary for the purposes of its legitimate interests as is necessary for the fulfilment of the contract with the cloud user and where such interests in data processing are not overridden by the interests or fundamental rights and freedoms of the data subject*". It is however not clear how it will be determined whether a processing activity is:

    - **both** (i) necessary for the purposes of the cloud provider's legitimate interests **and** (ii) necessary for the fulfilment of the contract with the cloud user, and therefore fulfilling criterion 13 (3); or

    - **either** (i) only necessary for the purposes of the cloud provider's legitimate interests **or** (ii) only necessary for the fulfilment of the contract with the cloud user, and therefore failing to fulfil criterion 13 (3).

Therefore, the Board recommends that criterion 13 is amended by adding further requirements to enable the above to be determined.

26. The Board takes note of the fact that the criteria 13 (1) and (3) covers situation where the cloud provider, as a controller, may process personal data in the pre- and post-contractual stages or for the performance of a contract, on the basis of Articles 6 (1) (b) and (f) GDPR, respectively. The EDPB recommends that draft criteria 13 (1) and (3) are amended in order to clarify which processing operations are covered in the pre- and post-contractual stage, for which the cloud provider is responsible as a controller, and that any explanatory text is amended accordingly.

27. Moreover, the circumstances in a controller-processor contractual relationship under which a cloud provider can process personal data of a cloud user as a controller appear to be limited. Despite this, the draft criteria 13 (1) and (3) states that the cloud provider may process personal data for the purposes of fulfilling its' contract as a controller, but it sets no limits under which circumstances a cloud provider may do so. The explanatory text of the criteria (p. 73p) clarifies that this covers fixing bugs, adhering to service-level agreements, direct communication with the user, and analysing access behaviour, etc. While the mentioned processing operations could possibly be undertaken by the cloud provider as a controller, it seems that several of those processing operations would, in the first place, be undertaken by the cloud provider as a processor. Therefore, the EDPB recommends to amend draft criteria 13 (1) and (3), to the effect that it is clarified that those criteria do not cover processing operations covered by the processing agreement with the cloud user. In addition, the EDPB encourages the introduction of a comprehensive list of which processing operations in the contractual relationship between the cloud provider and cloud user that are covered by draft criteria 13 (1) and (3).

2.5. GENERAL OBLIGATIONS FOR CONTROLLERS AND PROCESSORS

2.5.1 Obligations applicable to processors

28. The Board notes that in the draft criterion 10.1 (1), it states that "*approval is required only for sub-processes under which the further processor has the possibility to gain knowledge of processed personal data. Any sub-processing of personal data must not lead to a devaluation of the cloud user's right to object to changes in subcontracted processing*". This wording is confusing, and does not appear to be in line with Article 28(2) GDPR. The Board recommends to replace such wording with "In the case of general written authorisation, the cloud provider shall inform the cloud user of any intended changes concerning the addition or replacement of other processors, thereby giving the cloud user the opportunity to object to such changes".

29. The Board notices that in the draft criterion 10.1 (3), the criteria do not include the obligation of the processor, when engaging a sub-processor, to ensure that the same obligations as set out in the contract or other legal act between the controller and processor are imposed to the sub-processor, pursuant to Article 28(4) GDPR. Therefore, the Board recommends that the draft certification criteria are re-drafted accordingly to include this obligation.

30. In same section, draft criterion 10.1 on "further processors of the cloud provider (sub-processing)" it is mentioned that "the sub-processing may not complicate the protection of rights of data subjects". The Board is of the view that the way this criterion is drafted reduces the guarantees provided in Article 28 GDPR, thus recommends to either modify the wording of this criterion so to be in line with the GDPR or delete this part.

31. The Board notes in the draft criterion 9.2 and 19.2 on "data protection by default" the fact that the "cloud provider must ensure by default that personal data are not made accessible without individual's intervention to an indefinite number of natural persons and that no inappropriate risks arise for the data subject from providing in a too expansive extent access to personal data available". First, the Board considers that the wordings "inappropriate risks" and "too expansive extent" are unclear and should be further elaborated. These criteria should also clarify that the persons acting under the authority of the cloud provider shall access the data only on a need to know basis. Second, as far as criterion 9.2 and 19.2 are concerned, the Board highlights that controllers' obligations pursuant to Article 25(2) GDPR are not limited to data accessibility but shall also cover the amount of personal data collected, the extent of their processing, and the period of their storage. Consequently, the Board recommends to re-draft criteria 9.2 and 19.2 accordingly.

2.6 RISKS FOR THE RIGHTS AND FREEDOMS OF NATURAL PERSONS

32. The EDPB notes that the criteria 2.1 (1) is requiring the cloud provider to conduct a risk analysis with regards to data security. Furthermore, the criteria 2.1 (5) require that the cloud provider determine the data security measures to mitigate the risks it identifies.

    Other criteria are defined in the "Ensuring data security by appropriate state-of-the-art TOMs" section of the criteria catalogue. They further specify requirements on TOMs for several security aspects such as security zone and entry control (2.2), admission control (2.3), access control (2.4). For the purpose of clarity, the EDPB encourages to better differentiate the criteria that require the cloud provider:

- to take specific risk scenario into consideration when conducting a risk analysis with regards to data security (e.g. 2.2 (1) "*The cloud provider must ensure by means of risk-appropriate TOMs that its premises and facilities are protected against damage caused by acts of god"*)
- to implement mandatory TOMs (e.g. 2.2 (2) "*The cloud provider must control the physical entry to rooms and data processing facilities by means of a two-factor authentication procedure"*).

2.7 TECHNICAL AND ORGANISATIONAL MEASURES GUARANTEEING PROTECTION

33. The Board notes that criterion 16 related to notification of personal data breaches does not refer to the controller's obligations under Article 33(1) GDPR, in particular regarding the 72 hours delay. Further, criterion 16 states that the cloud user must notify the supervisory authority "**if** the personal data breach is unlikely to result in a risk to the rights and freedoms of the cloud user" while the GDPR states "**unless** the personal data [...]". Therefore the Board recommends to amend these criteria to ensure its' compliance with the GDPR.

34. With respect to section 2.5 (2) of the draft certification criteria on "*transfer of data and transport encryption*", the Board welcomes the inclusion of the criterion referring to "*whenever the transfer is encrypted, the encryption keys must be securely stored*". The Board is the opinion that the criterion shall further clarify how the encryption keys may be considered to be securely stored. The Board considers it important to have concrete and auditable criteria regarding security measures in place. Thus, the Board recommends that this criterion is modified accordingly.

35. Furthermore, in section No 2.7(1) on “pseudonymisation”, the Board notes that the cloud provider shall enable the cloud user to process data transferred in pseudonymised form. The Board highlights that this criterion gives the impression that pseudonymisation is limited to personal data transferred or transmitted. However, the Board is of the opinion that this is not in line with Article 32, which does not limit pseudonymisation to these two situations. Thus, the Board encourages that this criterion is modified accordingly.

36. With respect to section 2.8 (1) “Anonymisation”, for accuracy purposes, the Board recommends that the criterion referring to the cloud provider ensuring that anonymisation cannot be revoked, is modified and refers to TOMs being put in place to ensure that anonymisation cannot be reversed .

5 With respect to section No 2.9 on “Encrypting stored data”, the Board encourages to clarify that the storage includes backups of the stored data. Furthermore, regarding the “protection category one”, the Board considers that the criterion is unclear, potentially leading to different interpretations. If the criterion only applies to data encrypted by the cloud user before storing it on the cloud, the Board recommends to reformulate the sentence to capture this meaning only (for example: "The cloud provider must enable the cloud user to store data encrypted by the cloud user"). However, if the cloud provider offers encryption tools to the cloud user, then the cloud provider shall manage the cryptographic keys for encryption/decryption. The Board therefore encourages to clarify that “protection category one” cannot be selected by the applicant if its offer includes encryption tools to the cloud user because this protection level doesn’t cover secure key management.

2.8 CRITERIA FOR THE PURPOSE OF DEMONSTRATING THE EXISTENCE OF APPROPRIATE SAFEGUARDS FOR TRANSFER OF PERSONAL DATA

37. The Board welcomes draft criterion 11 on “data transfers”. However, the Board notes that the definitions referring to the “data importer” and “data exporter” are not corresponding to the ones provided either by the Board its Guidelines 05/2021 on the interplay between the application of Article 3 and the provisions on the international transfers as per Chapter V GDPR or by the European Commission in the standard contractual clauses for international transfers. Therefore, the Board, for consistency purposes, recommends to revise these definitions accordingly.

38. The Board could not identify specific criteria on transfers which would be applicable when the cloud provider acts as data controller. The Board recommends to add dedicated criteria to cover these situations.

39. In light of the considerations expressed above, the Board assumes that the draft criteria on transfers included in the scheme are only applicable to cloud providers acting as data processors. In this regard, the Board notes that, besides a generic reference to the “commissioned data processing agreement” with the controller, the draft criteria seem to consider the processor fully responsible for the assessment of the transfer tools to be used, the legislation of the third country as well as any supplementary measures to be adopted, where needed. On the contrary, according to Article 28(3)(a) GDPR, it should be recalled that 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 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 GDPR[5].

40. Therefore, the Board recommends to include a reference to the need for the processor to act 'in accordance with the instruction of the controller' notably in points 3 and 4 of the draft criterion 11.1 as well as in the explanation, implementation guidance and in the section concerning the European Essential Guarantees (in particular with regard to the reference to supplementary measures included in the paragraph concerning effective remedies[6].)

41. As for the access to the data transferred by public authorities of third countries, the draft criterion 11.1 in point 5 requires that the cloud provider discloses personal data only if the disclosure is based on an international agreement in force between the requesting third country and the EU or Germany. In such a case, the Board underlines that, in compliance with Article 28(3)(a) GDPR, the processor shall inform the controller of that legal requirement before any disclosures, unless that law prohibits such information on important grounds of public interest recognized in EU or German law, and recommends to amend the draft criterion accordingly

42. Moreover, the draft criterion 11.2 refers to cloud providers that do not have an establishment in the EU or the EEA but are nonetheless subject to the GDPR under Art. 3(2). Consequently, the Board understands that the certification scheme is applicable for certification customers that are established outside the EU or the EEA. Since this could imply that such a processor established outside the EU/EEA could also process personal data outside the EU/EEA, the Board recommends to clarify in the draft criterion 11.1 that whenever a "transfer" within the meaning of Article 44 GDPR to a processor established outside the EU or the EEA takes place, the obligations stipulated in Chapter V GDPR must be fully respected. In addition, the Board recommends to clarify that the applicant is not entitled to make use of the certification in a way that could give the impression that the certification itself is a transfer tool pursuant to Article 46 (2)(f) GDPR. Data controllers should, irrespective of the presence of the certification, nonetheless perform an assessment of the legislation of the host country before transferring data to the non-EU GDPR certified processor. In case the legislation does not provide for the appropriate level of protection, supplementary measures should be put in place. A data processor should refrain from applying for certification if they are aware that their legislation would prevent them from complying with the GDPR principles enshrined in the certification scheme[7].

[5] See the EDPB Guidelines 5/2021 on the interplay between the application of Article 3 and the provisions on international transfers as per Chapter V GDPR (paragraph 19)

[6] In that respect, the controller, according to Article 28(3)(a) GDPR, should be in a position to ask the processor to provide the assessment carried out with regard to the law and practice of the third country so as to verify whether the supplementary measures adopted by the processor effectively ensure an adequate level of protection of the personal data transferred in the third country.

[7] See the EDPB Opinion 25/2022 regarding the European Privacy Seal (EuroPriSe) certification criteria for the certification of processing operations by processors (paragraphs 9-11)

3 CONCLUSIONS / RECOMMENDATIONS

43. By way of conclusion, the EDPB considers that:

44. regarding the "general remarks" the Board recommends that the DE SA amends its draft decision approving the Auditor certification criteria for EU Cloud Service Data Protection to:

    1. specify in the criteria 9.2 and 19.2 what the term "inappropriate risks" entail and refer to the appropriate GDPR terminology.
    2. define in the criteria the terms "content or application data", "business", "consumer", "B2B", "B2C", "usage data", and "Commissioned Data Processing Agreement".
    3. replace the term "goods" when referring to "personal data as goods to be protected" with the term "information".
    4. modify criteria 2.2(3), 2.9.(4), 2.10(2), 2.5, 2.6(6), as they do not define a transparent level of data protection.

45. regarding the "scope of the certification mechanism and target of evaluation (TOE)", the Board recommends that the DE SA amends its draft decision approving the Auditor certification criteria for EU Cloud Service Data Protection to:

    1. further specify the scope of the scheme to (i) specified, explicit and legitimate categories of data processing operations where the cloud provider acts as a controller, and ii) examples of processing operations that can and cannot certified under the scheme.
    2. clarify in the criteria the situations in which the household/personal exemption would not apply to the cloud user who is a natural person.
    3. amend the scheme to make clear what adaptations are required to the certification criteria when the household/personal exemption is applicable vis-à-vis the cloud user (i.e. identify which criteria do not apply in this case or have specific criteria to cover this situation).
    4. further elaborate the criteria 8.1, 8.3 and 16 so to include the conditions for the non-applicability as defined by the GDPR.

46. regarding the "lawfulness of the processing" the Board recommends that the DE SA amends its draft decision approving the Auditor certification criteria for EU Cloud Service Data Protection to:

    1. replace the term "cloud user" in criteria 13 (1) with the term "data subject" and further amend the explanation part of these criteria.
    2. add further requirements in criterion 13 in order to determine when a processing activity is necessary for both (i) purposes of cloud provider's legitimate interest and (ii) fulfilment of the contract with the cloud user thus fulfilling the criterion 13(3) or necessary for only one of these two purposes.
    3. amend criteria 13(1) and (3) in order to clarify which processing operations are covered in the pre and post-contractual stage, for which the cloud provider is responsible as a controller and amend any explanatory text accordingly.
    4. amend criteria 13(1) and (3) to clarify that such criteria do not cover processing operations covered by the processing agreement with the cloud user.

47. regarding the "general obligations for controllers and processors" the Board recommends that the DE SA amends its draft decision approving the Auditor certification criteria for EU Cloud Service Data Protection to:

    1. amend the criterion 10.1(1) with regards to the use of sub-contractors by the cloud user so to bring it line with Article28 (2) GDPR.
    2. amend criterion 10.1 (3) so to include the obligation of the processor, when engaging a sub-processor to ensure that the same obligations, as set out in the contract of other legal act between the controller and the processor are imposed to the sub-processor, pursuant to Article 28(4) GDPR.
    3. either amend or delete the reference in the criterion 10.1 "the sub-processing may not complicate the protection of rights of data subject" as this reduces the guarantees of Article 28.
    4. amend the criteria 9(2) and 19(2) so further clarify the terms "inappropriate risks", "too expansive extent", the fact that the persons act until cloud service provider's authority shall access the data only on a need to know basis and that pursuant to Article 25(2) GDPR, controller's obligations are not limited data accessibility.

48. regarding the "technical and organisational measures guaranteeing protection" the Board recommends that the DE SA amends its draft decision approving the Auditor certification criteria for EU Cloud Service Data Protection to:

    1. amend criterion 16 in order to include controller's obligation to notify the supervisory authority within 72 hours and replace the term "if" with "unless" where referring to personal data breach which is unlikely to result in a risk to the rights and freedoms of the data subjects so to bring this criterion in line with Article 33 GDPR.
    2. further clarify criterion 2.5(2) to explain how the encryption keys may be considered to be securely stored.
    3. modify criterion 2.8(1) by adding that anonymisation cannot be revoked and by referring to TOMs being put in place to ensure that anonymisation cannot be reversed.
    4. amend criterion 2.9 and to include that the cloud provide shall enable the cloud user to store data encrypted by the latter.

49. regarding the "criteria for the purpose of demonstrating the existence of appropriate safeguards for transfer of personal data" the Board recommends the DE SA amends its draft decision approving the Auditor certification criteria for EU Cloud Service Data Protection to:

    1. align the definitions of the "data importer" and "data exporter" with either the ones of the EDPB Guidelines on the interplay between the application of Article 3 and the provisions on the international transfers as per Chapter V GDPR or the ones of the European Commission in the standard contractual clauses for international transfers.
    2. include a reference to the need for the processor to act 'in accordance with the instruction of the controller' notably in points 3 and 4 of the draft criterion 11.1 as well as in the explanation, implementation guidance and in the section concerning the European Essential Guarantees (in particular with regard to the reference to supplementary measures included in the paragraph concerning effective remedies.
    3. amend criterion 11.1 (point 5), including that the processor shall inform the controller of that about any disclose of personal data about this legal requirement, unless that law prohibits such information on important grounds of public interest recognised in EU or German law.

4. clarify in the draft criterion 11.1 that whenever a “transfer” within the meaning of Article 44 GDPR to a processor established outside the EU or the EEA takes place, the obligations stipulated in Chapter V GDPR must be fully respected.
5. clarify that the applicant is not entitled to make use of the certification in a way that could give the impression that the certification itself is a transfer tool pursuant to Article 46 (2)(f) GDPR.

4 FINAL REMARKS

This Opinion is addressed to the DE SA and will be made public pursuant to Article 64(5)(b) GDPR.

According to Article 64(7) and (8) GDPR, the DE SA shall communicate its response to this Opinion to the Chair by electronic means within two weeks after receiving the Opinion, whether it will amend or maintain its draft decision. Within the same period, it shall provide the amended draft decision or where it does not intend to follow the Opinion of the Board, it shall provide the relevant grounds for which it does not intend to follow this Opinion, in whole or in part.

Pursuant to Article 70(1)(y) GDPR, the DE SA shall communicate the final decision to the EDPB for inclusion in the register of decisions which have been subject to the consistency mechanism.

The EDPB recalls that, pursuant to Article 43(6) GDPR, the DE SA shall make public the Auditor certification criteria in an easily accessible form, and transmit them to the Board for inclusion in the public register of certification mechanisms and data protection seals, as per Article 42(8) GDPR.

For the European Data Protection Board
The Chair

(Anu Talus)