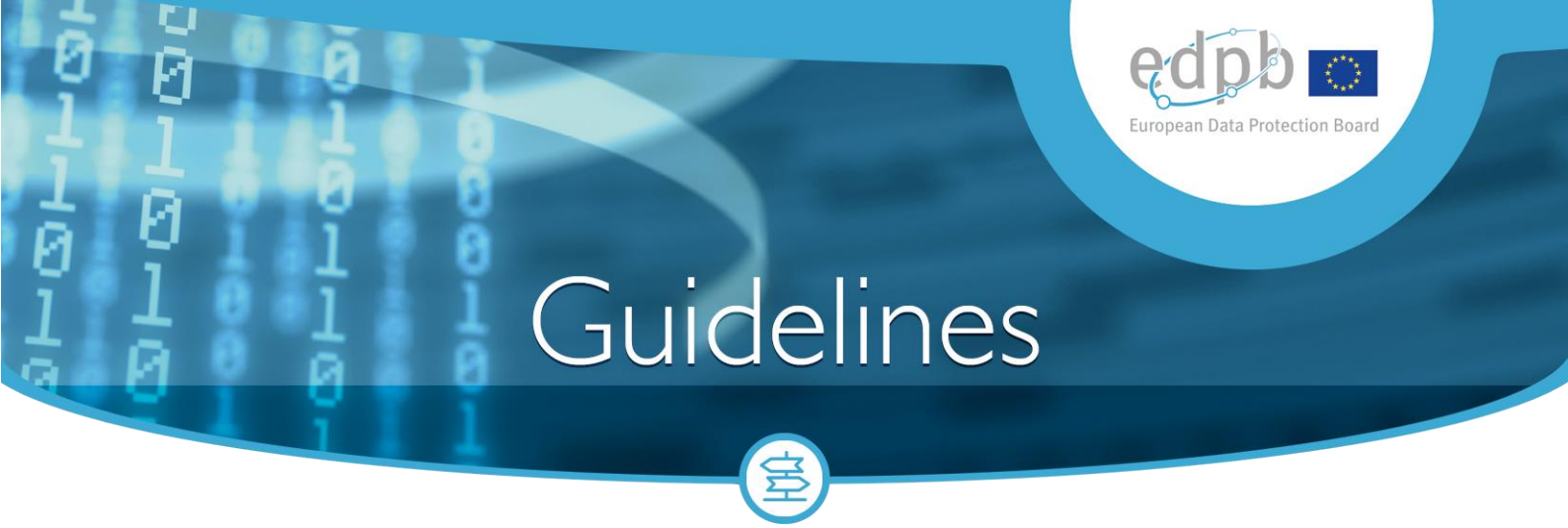

Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation

Version 3.0

4 June 2019

Adopted

Version history

Version 3.0	4 June 2019	Inclusion of Annex 2 (version 2.0 of Annex 2 adopted on 4 June 2019 after public consultation)
Version 2.1	9 April 2019	Adoption of a corrigendum to the Guidelines (paragraph 45)
Version 2.0	23 January 2019	Adoption of the Guidelines after public consultation - On the same date Annex 2 (version 1.0) was adopted for public consultation
Version 1.0	25 May 2018	Adoption of the Guidelines for publication consultation

Table of contents

The European Data Protection Board

Having regard to Article 70 (1e) 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,

Having regard to Article 12 and Article 22 of its Rules of Procedure of 25 May 2018,

Having considered the results of the public consultation on the guidelines that took place between 30 May 2018 and 12 July 2018, and on Annex 2 that took place between 15 February and 29 March 2019, as per Article 70 (4) of the GDPR

HAS ADOPTED THE FOLLOWING GUIDELINES

1 INTRODUCTION

1. The General Data Protection Regulation (Regulation 2016/279, 'the GDPR', or 'the Regulation'), provides a modernised, accountability and fundamental rights compliance framework for data protection in Europe. A range of measures that facilitate compliance with the provisions of the GDPR are central to this new framework. These include mandatory requirements in specific circumstances (including the appointment of Data Protection Officers and carrying out data protection impact assessments) and voluntary measures such as codes of conduct and certification mechanisms.

2. Before the adoption of the GDPR, the Article 29 Working Party established that certification could play an important role in the accountability framework for data protection.1 In order for certification to provide reliable evidence of data protection compliance, clear rules setting forth requirements for the provision of certification should be in place.2 Article 42 of the GDPR provides the legal basis for the development of such rules.

3. Article 42(1) of the GDPR provides that:

   "The Member States, the supervisory authorities, the [European Data Protection] Board and the European Commission shall encourage, in particular at the Union level, the establishment of data protection certification mechanisms and of data protection seals and marks, for the purpose of demonstrating compliance with this Regulation of processing operations by controllers and processors. The specific needs of micro, small and medium-sized enterprises shall be taken into account".

[1] Article 29 Working Party, Opinion 3/2010 on the principle of accountability, WP173, 13 July 2010, paragraphs 69-71.
[2] Article 29 Working Party Opinion 3/2010 on the principle of accountability (WP173), paragraph 69.

4. Certification mechanisms3 can improve transparency for data subjects, but also in business-to-business relations, for example between controllers and processors. Recital 100 of the GDPR states that the establishment of certification mechanisms can enhance transparency and compliance with the Regulation and allow data subjects to assess the level of data protection of relevant products and services.4

5. The GDPR does not introduce a right to or an obligation of certification for controllers and processors; as per Article 42(3), certification is a voluntary process to assist in demonstrating compliance with the GDPR. Member States and supervisory authorities are called to encourage the establishment of certification mechanisms and will determine the stakeholder engagement in the certification process and lifecycle.

6. Furthermore, the adherence to approved certification mechanisms is a factor supervisory authorities must consider as an aggravating or mitigating factor when deciding to impose an administrative fine and when deciding on the amount of the fine (Article 83.2(j)).5

1.1 Scope of the guidelines

7. These guidelines are limited in scope; they are not a procedural manual for certification in accordance with the GDPR. The primary aim of these guidelines is to identify overarching requirements and criteria that may be relevant to all types of certification mechanisms issued in accordance with Articles 42 and 43 of the GDPR. To this end, the guidelines:

    - explore the rationale for certification as an accountability tool;
    - explain the key concepts of the certification provisions in Articles 42 and 43; and
    - explain the scope of what can be certified under Articles 42 and 43 and the purpose of certification;
    - facilitate that the outcome of certification is meaningful, unambiguous, as reproducible as possible and comparable regardless of the certifier (comparability).

8. The GDPR allows for a number of ways for Member States and supervisory authorities to implement Articles 42 and 43. The guidelines provide advice on the interpretation and implementation of the provisions in Articles 42 and 43 and will help Member States, supervisory authorities and national accreditation bodies establish a more consistent, harmonised approach for the implementation of certification mechanisms in accordance with the GDPR.

9. The advice contained in the guidelines will be relevant for:

[3] These guidelines will refer to certification mechanisms and data protection seals and marks collectively as 'certification mechanisms', see section 1.3.2.
[4] Recital 100 states that the establishment of certification mechanisms should be encouraged to 'enhance transparency and compliance with the Regulation, allowing data subjects to quickly assess the level of data protection of relevant products and services'.
[5] See Article 29 Working Party, Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679 (WP 253).

- competent supervisory authorities and the European Data Protection Board ('the EDPB') when approving certification criteria under Article 42(5), Article 58(3)(f) and Article 70(1)(o);
- certification bodies when drafting and revising certification criteria prior to submission to the competent supervisory authority for approval as per Article 42(5);
- the EDPB when approving a European Data Protection Seal under Articles 42(5) and 70(1)(o);
- supervisory authorities, when drafting their own certification criteria;
- the European Commission, which is empowered to adopt delegated acts for the purpose of specifying the requirements to be taken into account for certification mechanisms under Article 43(8);
- the EDPB when providing the European Commission with an opinion on the certification requirements in accordance with Article 70(1)(q) and Article 43(8);
- national accreditation bodies, which will need to take into account certification criteria with a view to the accreditation of certification bodies in accordance with EN-ISO/IEC 17065/2012 and the additional requirements in accordance with Article 43; and
- controllers and processors when defining their own GDPR compliance strategy and considering certification as a means to demonstrate compliance.

10. The EDPB will publish separate guidelines to address the identification of criteria to approve certification mechanisms as transfer tools to third countries or international organisations in accordance with Article 42(2).

1.2 The purpose of certification under the GDPR

11. Article 42(1) provides that certification mechanisms shall be established "for the purpose of demonstrating compliance with this Regulation of processing operations by controllers and processors".

12. The GDPR exemplifies the context in which approved certification mechanisms may be used as an element to demonstrate compliance with obligations of the controllers and processors concerning:

- the implementation and demonstration of appropriate technical and organisational measures as referred in Articles 24(1),(3), 25, and 32(1), (3);
- sufficient guarantees (processor to controller) as referred to in paragraphs 1 and (sub-processor to processor) 4 of Article 28(5).

13. Since certification does not prove compliance in and of itself but rather forms an element that can be used to demonstrate compliance, it should be produced in a transparent manner. Demonstration of compliance requires supporting documentation, specifically written reports which not only repeat but describe how the criteria are met and if not initially met, describe the corrections and corrective actions and their appropriateness, thus providing the reasons

for granting and maintaining the certification. This includes the outline of the individual decision for granting, renewing, or withdrawing of a certificate. It should provide the reasons, arguments, and proofs resulting from the application of criteria and the conclusions, judgments, or inferences from facts or premises collected during certification.

1.3 Key concepts

14. The following section explores the key concepts in Articles 42 and 43. This analysis develops an understanding of basic terms and the scope of certification under the GDPR.

1.3.1 Interpretation of "certification"

15. The GDPR does not define "certification". The International Standards Organisation (ISO) provides a universal definition of certification as "the provision by an independent body of written assurance (a certificate) that the product, service or system in question meets specific requirements." Certification is also known as "third party conformity assessment" and certification bodies can also be referred to as "conformity assessment bodies" (CABs). In EN-ISO/IEC 17000:2004 - Conformity assessment -- Vocabulary and general principles (to which ISO17065 refers) - certification is defined in the following terms: "third party attestation… related to products, processes, and services".

16. Attestation is an 'issue of a statement, based on a decision following review, that fulfilment of specific requirements has been demonstrated' (section 5.2, ISO 17000:2004).

17. In the context of certification under Articles 42 and 43 of the GDPR, certification shall refer to third party attestation related to processing operations by controllers and processors.

1.3.2 Certification mechanisms, seals and marks

18. The GDPR does not define "certification mechanisms, seals or marks" – and uses the terms collectively. A certificate is a statement of conformity. A seal or mark can be used to signify the successful completion of the certification procedure. A seal or mark commonly refers to a logo or symbol whose presence (in addition to a certificate) indicates that the object of certification has been independently assessed in a certification procedure and conforms to specified requirements, stated in normative documents such as regulations, standards or technical specifications. These requirements in the context of certification under the GDPR are set out in the additional requirements that supplement the rules for accreditation of certification bodies in EN-ISO/IEC 17065/2012 and the certification criteria approved by the competent supervisory authority or the Board. A certificate, seal or mark under the GDPR can only be issued following the independent assessment of evidence by an accredited certification body or competent supervisory authority, stating that the certification criteria have been satisfied.

19. The table provides a generic example of a certification process.

Submission of application by controller or processor	Formal Check by CB	Assessment Pre-Evaluation	Assessment Evaluation of ToE	Assessment Validation of results	Information to CSA	Certification	Monitoring	Renewal of certification
Is the description of the target of evaluation (ToE) anambigous and complete including interfaces?	Can the ToE description be accepted?	What are the applicable criteria?	Does the ToE meet the criteria?	Are all relevant criteria specified reflecting the ToE?	Have the reasons for granting or withdrawing certification been provided?	Can the certificate be awarded?	Does the ToE continue to meet the criteria	Does the processing still meet the certification criteria?
Can access to the ToE processing activities be granted?	Are all documents complete and up -to - date?	What are the applicable evaluation methods?	Is the documentation of the ToE correct?	Has the evaluation been sufficiently documented ?		Are the reports ready for publishing?	Is the certificate/seal/trust mark used correctly?	Have areas of development been satisfactorily addressed?
Art. 42(6)	Art. 43(4)	Art. 43(4)	Art. 42(5), Art. 43(4)	Art. 43(4)	Art. 43(1), 43(5)	Art. 43(1); Art. 42 (7)	Art. 42 (7)	Art. 42 (7)

2 THE ROLE OF THE SUPERVISORY AUTHORITIES

20. Article 42(5) provides that certification shall be issued by an accredited certification body or by a competent supervisory authority. The GDPR does not make the issuance of certifications a mandatory task of the supervisory authorities. Instead, the GDPR allows for a number of different models. For example, a supervisory authority may decide for one or more of the following options:

    - issue certification itself, in respect of its own certification scheme;
    - issue certification itself, in respect of its own certification scheme, but delegate whole or part of the assessment process to third parties;
    - create its own certification scheme, and entrust certification bodies with the certification procedure which issue the certification; and
    - encourage the market to develop certification mechanisms.

21. A supervisory authority will also have to consider its role in the light of the decisions made at the national level concerning accreditation mechanisms – in particular if the supervisory authority itself is empowered to accredit certification bodies under Article 43(1) GDPR. Thus each supervisory authority will determine which approach to take in order to pursue the broad intent of certification under the GDPR. This will be determined in the context of not only the tasks and powers in Articles 57 and 58, but also in accounting for certification as a factor to be taken into account in determining administrative fines, and more generally as a means of demonstrating compliance.

2.1 Supervisory Authority as certification body

22. Where a supervisory authority chooses to conduct certification, it will have to carefully assess its role with respect to its assigned tasks under the GDPR. Its role should be transparent in the exercise of its functions. It will need to give consideration specifically to the separation of powers relating to investigations and enforcement in order to avoid any potential conflicts of interest.

23. When acting as a certification body a supervisory authority will have to ensure the proper set up of a certification mechanism and develop its own or adopt certification criteria. In addition, every supervisory authority which issues certifications has the task to periodically review them (Article 57(1)(o)) and the power to withdraw them where the requirements for certification are not or no longer met (Article 58(2)(h)). To meet these requirements, it is useful to set up a certification procedure and process requirements, and, if not stipulated otherwise e.g. by national law, put in place a legally enforceable agreement for the provision of certification activities with the individual applicant organisation. It should be ensured that this certification agreement requires the applicant to comply at least with the certification criteria including necessary arrangements to conduct the evaluation, monitoring adherence to the criteria, and periodic review including access to information and/or premises, documentation and publication of reports and results, and investigation of complaints. Further, it is expected that a supervisory authority will follow the requirements in the guidelines for accreditation of certification bodies in addition to the requirements pursuant to Article 43(2).

2.2 Supervisory Authority's further tasks regarding certification

24. In Member States where certification bodies become active, the supervisory authority has the power and task irrespective of its own activities:

    - to assess a certification scheme's criteria and make a draft decision (Article 42(5));
    - to communicate to the Board the draft decision when it intends to approve the criteria for certification (Article 64(1)(c), 64(7)) and consider the Board's opinion (Article 64(1)(c) and 70(1)(t));
    - to approve the criteria for certification (Article 58(3)(f)) before accreditation and certification can take place (Article 42(5) and 43(2)(b));
    - to publish the certification criteria (Article 43(6);
    - to act as competent authority for EU wide certification schemes, which may result in an EDPB approved European Data Protection Seals (Articles 42(5) and Article 70(1)(o); and
    - to order a certification body (a) not to issue certification or (b) to withdraw certification where the requirements for certification (certification procedures or criteria) are not or are no longer met (Article 58(2)(h).

25. The GPDR tasks the supervisory authority with approving certification criteria but not with developing criteria. In order to approve certification criteria under Article 42(5), a supervisory authority should have a clear understanding of what to expect, specifically in terms of scope and content for demonstrating compliance with the GDPR and with regard to its task to monitor and enforce the application of the regulation. The annex provides guidance to ensure a harmonized approach when assessing criteria for the purpose of approval.

26. Article 43(1) requires certification bodies to inform their supervisory authority before issuing or renewing certifications to allow the competent supervisory authority to exercise its corrective powers under point (h) of Article 58(2). Additionally, Article 43(5) also requires certification bodies to provide the competent supervisory authority with the reasons for granting or withdrawing the requested certification. Although the GDPR allows for supervisory authorities to determine how to receive, acknowledge, review and deal with this information operationally (for example, this could include technological solutions to enable reporting by certification bodies), a process and criteria to process the information and reports provided on each successful certification project by the certification body according to Article 43(1) may be put in place. On the basis of this information, the supervisory authority can exercise its power to order the certification body to withdraw or not issue a certification (Article 58(2)(h)) and to monitor and enforce the application of the requirements and criteria of certification under the GDPR (Article 57(1)(a) and 58(2)(h)). This will support a harmonized approach and comparability in certification by different certification bodies and that information about an organisation's certification status is known by supervisory authorities.

3 THE ROLE OF A CERTIFICATION BODY

27. A certification body's role is to issue, review, renew, and withdraw certifications (Article 42(5), (7)) on the basis of a certification mechanism and approved criteria (Article 43(1)). This requires the certification body or a certification scheme owner to determine and set up certification criteria and certification procedures, including procedures for monitoring of adherence, reviewing, handling complaints, and withdrawal. The certification criteria are reviewed as part of the accreditation process, which considers the rules and procedures under which certifications, seals, or marks are issued (Article 43(2)(c)).

28. The existence of a certification mechanism and certification criteria are necessary for the certification body to achieve accreditation under Article 43. A major impact on what a certification body does arises from the scope and type of certification criteria which have an impact on the certification procedures and vice versa. Specific criteria may for example require specific methods of evaluation, such as on-site inspections and code review. These procedures are mandatory for accreditation and are further explained in the guidelines on accreditation.

29. The certification body is required by the GDPR to provide supervisory authorities with information, especially on individual certifications, which is necessary to monitor the application of the certification mechanism (Article 42(7), 43(5), 58(2)(h)).

4 THE APPROVAL OF CERTIFICATION CRITERIA

30. The certification criteria form an integral part of any certification mechanism. Consequently, the GDPR requires the approval of certification criteria of a certification mechanism by the competent supervisory authority (Articles 42(5) and 43(2)(b)). Or in the case of a European Data Protection Seal, certification criteria is approved by the EDPB (Articles 42(5) and 70(1)(o)). Both routes for approval of certification criteria are explained below.

31. The EDPB recognizes the following purposes for approval of certification criteria:

    - to properly reflect the requirements and principles concerning the protection of natural persons with regard to the processing of personal data laid down in Regulation (EU) 2016/679; and
    - to contribute to the consistent application of the GDPR.

32. Approval is granted on the basis of the GDPR requirement that the certification mechanism enables controllers and processors to demonstrate compliance with the GDPR is fully reflected in the certification criteria.

4.1 Approval of criteria by the competent supervisory authority

33. Certification criteria must be approved by the competent supervisory authority prior or during the accreditation process for a certification body. Approval is also required for updated or additional schemes or sets of criteria under ISO 17065 by the same certification body, prior to their use of the amended certification mechanisms (Articles 42(5) and 43(2)(b)). Supervisory authorities shall treat all requests for approval of certification criteria in a fair and non-discriminatory way, according to a publicly available procedure specifying the general conditions to be met and the description of the approval process.

34. A certification body can only issue certification in a particular Member State in accordance with the criteria approved by the supervisory authority in that Member State. In other words, certification criteria need to be approved by the competent supervisory authority where the certification body aims to offer certification and obtains the accreditation. See the section below for European wide certification schemes.

4.2 Approval of criteria by EDPB for the European Data Protection Seal

35. A certification body can also issue certification in accordance with criteria approved by the EDPB for a European Data Protection Seal. Certification criteria approved by the EDPB pursuant to Article 63 may result in a European Data Protection Seal (Article 42(5)). In light of existing certification and accreditation conventions, the EDPB acknowledges that it is desirable to avoid fragmentation of the data protection certification market. It notes that Article 42(1) provides that Member States, supervisory authorities, the Board and the Commission shall encourage the establishment of certification mechanisms, in particular at Union level.

4.2.1 Application for approval

36. The application for approval of criteria pursuant to Article 42(5) and 70(1)(o), by the EDPB must be submitted through a competent supervisory authority and should state the intention of the scheme owner, candidate or accredited certification body to offer the criteria in a certification mechanism addressing controllers and processors in all Member States. The competent supervisory authority will provide a draft to the EDPB when it considers that the criteria could be approved by the EDPB.

37. The choice of where to submit an application for approval of criteria will be based on the certification scheme owners or the certification bodies headquarters.

38. If a certification body submits an application, it would normally be in the process of applying for accreditation or already accredited by either the competent supervisory authority or the national accreditation body of its Member State. Where the certification body is already accredited for a GDPR certification mechanism, this may help streamline the approvals process.

4.2.2 European Data Protection Seal criteria

39. The EDPB will co-ordinate the assessment process and approve the European Data Protection Seal criteria as required. The assessment will address such areas as: the criteria's scope and the ability to serve as a common certification. Where the criteria are approved by the EDPB, the competent supervisory authority for the EU headquarters of the certification body is expected to handle complaints about the mechanism itself and inform the other supervisory authorities. This supervisory authority is also competent to take measures against the certification body. As the case may be, the competent supervisory authority will notify the other supervisory authorities and the EDPB.

40. Certification criteria addressing a common certification are subject to EU-wide demands and should provide a specific mechanism to cope with these demands. European certification mechanisms must be intended for use in all Member States. Based on Article 42(5) the mechanism for a European Data Protection Seal as well as its criteria needs to be customisable in a way as to take into account national sector specific regulations where applicable, e. g., for data processing in schools and shall envisage a European-wide application.

41. Example: An international School offering schooling to data subjects in the Union is based in Member State "A". The school wishes to certify its online application process with an EU-wide certification scheme to earn a European Data Protection Seal. This school aims to apply for certification of processing operations offered by a certification body established in Member State "B" on the basis of a European Data Protection Seal. The Seal criteria designed and documented in the relevant mechanism must be able to take into account the regulations for schools applicable in Member State "A". The criteria should also require the school's online application process to provide information and take account of the applicable Member State data protection requirements that may differ in other Member States An example is sets of personal data to be submitted for application purposes, e.g. kindergarten grades or test

results, differing retention periods, collection or processing of financial or biometric data, further processing limitations.

- High level criteria for approval of a European Data Protection Seal mechanism include:
  - criteria approved by the Board;
  - application across jurisdictions reflecting where appropriate national legal requirements and sector specific regulations;
  -
- harmonised criteria which are customisable to reflect national requirements;
  - description of the certification mechanism specifying;
  - the certification agreements, recognizing pan-European requirements;
  - procedures to ensure and provide solutions for national variance and ensure the Seal helps demonstrate GDPR compliance; and
  - the language of the reports addressing all affected supervisory authorities.

42. The annex also contains advice on the European Data Protection Seal criteria.

4.2.3 Role of accreditation

43. As noted in 4.2.1, when criteria are identified as being suitable for common certification, and have been approved as such by the Board pursuant to Article 42(5), then certification bodies may be accredited to conduct certification under these criteria at Union level.

44. Schemes that are intended only to be offered only in particular Member States will not be candidates of EU Seals. Accreditation for the scope of a European Data Protection Seal will require accreditation in the Member State of the headquarters of the certification body intending to operate the scheme, i.e. responsible for issuing certifications and managing the certification activities of its entities and subsidiaries in other Member States. Where other establishments or offices manage and perform certifications autonomously, each of these establishments or offices will require separate accreditation in the Member State where they are based. In other words, accreditation is necessary only in the Member State of the headquarters of the certification body when only the headquarters issue the certificates. By contrast, when other establishments of the certification body also issue certificates, these establishments need to be accredited as well.

45. Consequently, if a certification body has not been accredited to certify under the European Data Protection Seal, then the EDPB approved criteria cannot be used and the Seal cannot be offered.

5 THE DEVELOPMENT OF CERTIFICATION CRITERIA

46. The GDPR established the framework for the development of certification criteria. Whereas fundamental requirements concerning the procedure of certification are addressed in Articles 42 and 43 while also providing essential criteria for certification procedures, the basis for certification criteria must be derived from the GDPR principles and rules and help to provide assurance that they are fulfilled.

47. The development of certification criteria should focus on verifiability, significance, and suitability of certification criteria to demonstrate compliance with the Regulation. The certification criteria should be formulated in such a way that they are clear and comprehensible and that they allow practical application.

48. When drafting certification criteria the following compliance aspects in support of the assessment of the processing operation, inter alia, shall be taken into account, where applicable:

    - the lawfulness of processing pursuant to Article 6;
    - the principles of data processing pursuant to Article 5;
    - the data subjects' rights pursuant to Articles 12-23;
    - the obligation to notify data breaches pursuant to Article 33;
    - the obligation of data protection by design and by default, pursuant to Article 25;
    - whether a data protection impact assessment, pursuant to Article 35(7)(d) has been conducted, if applicable; and
    - the technical and organisational measures put in place pursuant to Article 32.

49. The extent to which these considerations are reflected in the criteria may vary depending on the scope of certification which may include the type of processing operation(s) and the area (e.g. health sector) of certification.

5.1 What can be certified under the GDPR?

50. The EDPB considers that the GDPR provides a broad scope for what can be certified under the GDPR, as long as the focus is on helping demonstrate compliance with this Regulation of processing operations by controllers and processors (Article 42.1).

51. When assessing a processing operation, the following three core components must be considered, where applicable:

    1. personal data (material scope of the GDPR);
    2. technical systems - the infrastructure, such as hardware and software, used to process the personal data; and

3. processes and procedures related to the processing operation(s).

52. Each component used in processing operations must be subject to assessment against the set criteria. At least four different significant factors can be of influence: 1) the organisation and legal structure of the controller or processor; 2) the department, environment and people involved in the processing operation(s); 3) the technical description of the elements to be assessed; and finally 4) the IT infrastructure supporting the processing operation including operating systems, virtual systems, databases, authentication and authorization systems, routers and firewalls, storage systems, communication infrastructure or Internet access and associated technical measures.

53. All three core components are relevant for the design of certification procedures and criteria. Depending on the object of certification the extent to which they are taken into account may vary. For example, in some cases, some components can be disregarded if they are judged not relevant to the object of the certification.

54. To further specify what may be certified under the GDPR, the GDPR contains additional guidance. It follows from Article 42.7 that certifications under the GDPR are issued only to data controllers and data processors, which rule out for instance the certification of data protection officers. Art. 43(1)(b) refers to ISO 17065 which provides for the accreditation of certification bodies assessing the conformity of products, services and processes. A processing operation or a set of operations may result in a product or service in the terminology of ISO 17065 and such can be subject of certification. For instance, the processing of employee data for the purpose of salary payment or leave management is a set of operations within the meaning of the GDPR and can result in a product, process or a service in the terminology of ISO.

55. On the basis of these considerations, the EDPB considers that the scope of certification under the GDPR is directed to processing operations or sets of operations. These may comprise of governance processes in the sense of organisational measures, hence as integral parts of a processing operation (e.g. the governance process established for complaints handling as part of the processing of employee data for the purpose of salary payment).

56. In order to assess the compliance of the processing operation with the certification criteria, a use case must be provided. For example, compliance of the use of a technical infrastructure deployed in a processing operation depends on the categories of data it is designed to process. Organisational measures depend on the categories and amount of data and the technical infrastructure used for processing, taking into account the nature, scope, content and purposes of the processing as well as the risks to the rights and freedoms of the data subjects.

57. Moreover, it must be kept in mind that IT applications can differ widely even though serving the same processing purposes. Therefore, this must be considered when defining the scope of the certification mechanisms and drafting the certification criteria, i.e. the scope of certification and criteria should not be so narrow as to exclude IT applications designed differently.

5.2 Determining the object of certification

58. The scope of a certification mechanism is to be distinguished from the object - also called the target of evaluation (ToE) - in individual certification projects under a certification mechanism. A certification mechanism can define its scope either generally or in relation to a specific type or area of processing operations and can thus already identify the objects of certification that fall within the scope of the certification mechanism (e.g. secure storage and protection of personal data contained in a digital vault). At any instance, a reliable, meaningful assessment of conformity can take place only if the individual object of a certification project is described precisely. It must be described clearly which processing operations are included in the object of certification and then the core components, i.e. which data, processes and technical infrastructure, will be assessed and which will not. In doing so, the interfaces to other processes must always be considered and described as well. Clearly, what is not known cannot be part of the assessment and thus cannot be certified. In any case, the individual object of certification must be meaningful with respect to the message or claim made on/by the certification and should not mislead the user, customer or consumer.

59. [Example 1]

A bank offers to its customers a website for the purpose of online banking. In the framework of this service, there is the possibility to make transfers, buy shares, initiate standing orders and manage the account. The bank wishes to certify the following under a data protection certification mechanism with a general scope based on generic criteria:

a) Secure log-in

Secure log-in is a processing operation which is understandable for the end user and which is relevant from a data protection perspective since it plays an important part in ensuring the security of personal data involved. Therefore, this processing operation is necessary for secure log-in and can thus constitute a meaningful ToE if the certificate states clearly that only the log-in processing operation is certified.

b) Web front-end

Whilst the web front-end can be relevant from a data protection perspective it is not understandable by the end user and therefore cannot be a meaningful ToE. Moreover, it is not clear to the user which services on the website and thus which processing operations are covered by the certification.

c) Online banking

The web front end together with the back-end are processing operations provided within the online banking service which can be meaningful to the user. In this context, both must be included in the ToE. Whereas processing operations that are not directly connected to the provision of the online banking service, such as processing operations for the purpose of prevention of money laundering, can be excluded from the ToE.

However, the online-banking services offered by the bank via its website may also include other services which in turn require their own processing operations. In this context, other services may include, for example, the offering of an insurance product. Since this additional

service is not directly connected with the purpose of providing online banking services, it can be excluded from the ToE. If this additional service (insurance) is excluded from the ToE, the interfaces for this service integrated on the website are part of the ToE and must therefore be described in order to clearly distinguish between the services. Such a description is necessary to identify and evaluate possible data flows between the two services.

60. [Example 2]

    A bank offers to its customers a service allowing them to aggregate the information related to different accounts and credit cards from several banks (account aggregation). The bank wishes to have its service certified under the GDPR. The competent supervisory authority has approved a specific set of certification criteria focusing on this type of activity. The scope of the certification mechanism only addresses the following compliance aspects:

    - user authentication; and
    - acceptable ways to obtain the data to be aggregated from other banks/services.

    Since the scope of this certification mechanism defines the ToE by itself, it is not possible to meaningfully narrow down the ToE under the proposed scope and certify only specific features or a single processing activity. In this scenario, a ToE must equal a specific scope.

5.3 Evaluation methods and methodology of assessment

61. A conformity assessment to help demonstrate compliance of processing operations requires identifying and determining the methods for evaluation and the methodology of assessment. It matters whether the information for the assessment is collected from documentation only (which would not be sufficient in itself) or whether it is actively collected on site and by direct or indirect access. The way in which information is collected has consequences for the significance of certification and should therefore be defined and described.

    Procedures for the issuance and periodic review of certifications should include specifications to identify the appropriate level of evaluation (depth and granularity) to meet the certification criteria and should include the provision of:

    - information about and specification of the applied assessment methods and findings collected e.g. during on site audits or from documentation,
    - evaluation methods focusing on the processing operations (data, systems, processes) and the purpose of processing,
    - identification of the categories of data, the protection needs and whether processors or third parties are involved,
    - identification of roles and existence of an access control mechanism defined around roles and responsibilities.

62. The depth of evaluation has an impact on the significance and value of the certification. By reducing the depth of evaluation for pragmatic purposes or to reduce the costs, the significance of a data protection certification will be diminished. Decisions on the granularity of the evaluation on the other hand, may exceed the financial capabilities of the applicant and

often the capability of evaluators and auditors, too. For purposes of demonstrating compliance it may not always be crucial to reach a very detailed analysis of the IT systems used to remain meaningful.

5.4 Documentation of assessment

63. Certification documentation should be thorough and comprehensive. A lack of documentation means that a proper assessment cannot take place. The essential function of certification documentation is that it provides for transparency in the evaluation process under the certification mechanism. Documentation delivers answers to questions concerning the requirements set out by law. Certification mechanisms should provide for a standardized documentation methodology. Thereafter evaluation will allow comparison of the certification documentation with the actual status on-site and against the certification criteria.

64. Comprehensive documentation of what has been certified and the methodology used serves transparency. Pursuant to Article 43(2)(c), certification mechanisms should establish procedures that allow the review of certifications. In order to allow the supervisory authority to assess whether and to what extent the certification can be acknowledged in formal investigations, detailed documentation may be the most appropriate means to communicate. The documentation produced during evaluation should therefore focus on three main aspects:

    - consistency and coherence of evaluation methods executed;
    - evaluation methods directed to demonstrate compliance of the certification object with the certification criteria and thus with the Regulation; and
    - that the results of evaluation have been validated by an independent and impartial certification body.

5.5 Documentation of results

65. Recital 100 provides information on the objectives pursued with the introduction of certification.

"In order to enhance transparency and compliance with this Regulation, the establishment of certification mechanisms and data protection seals and marks should be encouraged, allowing data subjects to quickly assess the level of data protection of relevant products and services."

66. To enhance transparency the documentation and communication of results play an important role. Certification bodies using certification mechanisms, seals or marks directed towards the data subjects (in their roles as consumers or customers) should provide easily accessible, intelligible and meaningful information about the certified processing operation(s). This public information should include at least the

    - description of the ToE;
    - reference to the approved criteria applied to the specific ToE;

- the methodology for the evaluation of the criteria (on-site evaluation, documentation, etc.); and
- the duration of the validity of the certificate; and
- should allow comparability of results for supervisory authorities and the public.

6 GUIDANCE FOR DEFINING CERTIFICATION CRITERIA

67. Certification criteria are an integral part of a certification mechanism. The certification procedure includes the requirements of how, by whom, to what extent and the granularity of the assessment which shall take place in individual certification projects concerning a specific object or target of evaluation (ToE). The certification criteria provide the nominal requirements against which the actual processing operation defined in the ToE is assessed. These guidelines for defining certification criteria provide generic advice that will facilitate the assessment of certification criteria for the purpose of approval.
    - The following general considerations should be taken into account when approving or defining certification criteria. Certification criteria should:
    - be uniform and verifiable,
    - auditable in order to facilitate the evaluation of processing operations under the GDPR, by specifying in particular, the objectives and the implementing guidance for achieving those objectives;
    - be relevant with respect to the targeted audience (e.g. B2B and business to customer (B2C);
    - take into account and where appropriate be inter-operable with other standards (such as ISO standards, national level standards); and
    - be flexible and scalable for application to different types and sizes of organisations including micro, small and medium sized enterprises in accordance with Article 42(1) and the risk-based approach in accordance with Recital 77.
68. A small local company, such as a retailer, will usually carry out less complex processing operations than a large multinational retailer. While the requirements for the lawfulness of the processing operations are the same, the scope of data processing and its complexity must be taken into account; it follows that there is a need for certification mechanisms and their criteria to be scalable according to the processing activity in question.

6.1 Existing standards

69. Certification bodies will need to consider how specific criteria take existing relevant instruments, such as Codes of Conducts, technical standards or national regulatory and legal

initiatives into account. Ideally, criteria will be interoperable with existing standards that can help a controller or processor meet their obligations under the GDPR. However, while industry standards often focus on the protection and security of the organisation against threats, the GDPR is directed at the protection of fundamental rights of natural persons. This different perspective must be taken into account when designing criteria or approving criteria or certification mechanisms based on industry standards.

6.2 Defining criteria

70. Certification criteria must correspond to the certification statement (message or claim) of a certification mechanism or scheme and match the expectations it raises. The name of a certification mechanism may already identify the scope of application and will have consequences for the determination of criteria.

71. [Example 3]

    A mechanism called "HealthPrivacyMark" should limit its scope to the health sector. The seal name raises the expectation that data protection requirements in connection with health data have been examined. Accordingly, the criteria of this mechanism must be adequate for assessing data protection requirements in this sector.

72. [Example 4]

    A mechanism that relates to the certification of processing operations comprising governance systems in data processing should identify criteria that allow for the recognition and assessment of governance processes and its supporting technical and organisational measures.

73. [Example 5]

    The criteria for a mechanism that relates to cloud computing needs to take account of the special technical requirements necessary for the use of cloud-based services. For instance, if servers are used outside the EU, the criteria must consider the conditions laid down in Chapter V of the GDPR with respect to data transfers to third-countries.

74. Criteria designed to fit different ToEs in different sectors and/or Member States should: allow an application to different scenarios; allow identification of the adequate measures to fit small, medium, or large processing operations and reflect the risks of varying likelihood and severity to the rights and freedoms of natural persons in line with the GDPR. Consequently, the certification procedures (e.g. for documentation, testing, or evaluation method and depth) complementing the criteria must respond to these needs and allow and have rules in place, for example to apply the relevant criteria in individual certification projects. Criteria must facilitate an assessment as to whether sufficient guarantees for the implementation of appropriate technical and organisational measures have been provided.

6.3 Lifetime of certification criteria

75. Even though certification criteria must be reliable over time they should not be carved in stone. They shall be subject to revision for instance where:

    - the legal framework is amended;
    - terms and provisions are interpreted by judgments of the European Court of Justice; or
    - the technical state of the art has evolved.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

ANNEX 1: TASKS AND POWERS OF SUPERVISORY AUTHORITIES IN RELATION TO CERTIFICATION IN ACCORDANCE WITH THE GDPR

	Provisions	Requirements
Tasks	Article 43(6)	Requires the supervisory authority to make public the criteria referred to in Article 42(5) in an easily accessible form and transmit them to the Board.
	Article 57(1)(n)	Requires the supervisory authority to approve certification criteria pursuant to Article 42(5).
	Article 57(1)(o)	Provides that where appropriate (i.e. where it issues certification), it shall carry out a periodic review of certification issued in accordance with Article 42(7).
	Article 64(1)(c)	Requires the supervisory authority to communicate the draft decision to the Board, when it aims to approve the criteria for certification referred to in Article 42(5).
Powers	Article 58(1)(c)	Provides that the supervisory authority has the power to carry out reviews of certification pursuant to Article 42(7);
	Article 58(2)(h)	Provides that the supervisory authority has the power to withdraw or order the certification body to withdraw certification or order the certification body not to issue certification.
	Article 58(3)(e)	Provides that the supervisory authority has the power to accredit certification bodies
	Article 58(3)(f)	Provides that the supervisory authority has the power to issue certification and approve certification criteria.
	Article 58(3)(e)	Provides that the supervisory authority has the power to accredit certification bodies.
	Article 58(3)(f)	Provides that the supervisory authority has the power to issue certification and approve certification criteria.

ANNEX 2

1 INTRODUCTION

Annex 2 provides guidance for review and assessment of certification criteria pursuant to Article 42(5). It identifies topics that a data protection supervisory authority and the EDPB will consider and apply for the purpose of approval of certification criteria of a certification mechanism. The questions should be considered by certification bodies and scheme owners who wish to draft and present criteria for approval. The list is not exhaustive, but presents the minimum topics to be considered. Not all questions will be applicable; however they should be considered when drafting criteria and reasoning may be needed to explain why criteria do not cover specific aspects. Some questions are repeated, as they are from different perspectives. This guidance should be considered in accordance with the legal requirements provided by the GDPR and, where applicable, by national legislation.

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

a. Is the scope of the certification mechanism (for which the data protection criteria shall be used) clearly described?

b. Is the scope of the certification mechanism meaningful to its addressed audience and not misleading?

- *Example: A "Trusted Company Seal" suggests that the processing activities of an entire company have been audited, even though only specified processing operations, e.g. the online payment process, are actually subject to certification. The scope is therefore misleading.*

c. Does the scope of the certification mechanism reflect all relevant aspects of the processing operations?

- *Example: A "Privacy Health Mark" must include all evaluation data concerning health in order to address requirements pursuant to Article 9.*

d. Does the scope of the certification mechanism allow meaningful data protection certification taking into account the nature, the content, the risk of the related processing operations?

- *Example: If the scope of the certification mechanism focuses only on specific aspects of processing operations, such as the collection of data, but not on the further processing operations, such as processing for the purpose of creating advertising profiles or the management of data subject's rights, would not be meaningful for data subjects.*

e. Does the scope of the certification mechanism cover personal data processing in the relevant country of application or does it address cross border processing and/or transfers?

f. Do the certification criteria sufficiently describe how the ToE should be defined?

- *Example: A "Privacy Seal" offering a general scope only requiring "a specification of the processing subject to certification" would not provide clear enough guidance on how to set and describe a ToE.*

- *Example: A (specific) scope, "The Privacy Vault Seal", addressing secure storage should describe in detail the requirements to meet this scope in its criteria, e.g. definition of vault, system requirements, mandatory technical and organisational measures (TOMs). In that case the scope can clearly define the ToE.*

    (1) Do the criteria require the ToE to include an identification of all relevant processing operations, illustration of data flows and a determination of the ToE's area of application?

    - *Example: A certification mechanism offers certification of processing operations of controllers under the GDPR without specifying further the area of application (general scope). The criteria used by the mechanism requires the applicant controller to determine the targeted processing operation (ToE) in terms of data types, systems and processes deployed.*

    (2) Do the criteria require from the applicant to make clear where the processing that is subject to evaluation starts and ends? Do the criteria require the ToE to include interfaces where interdependent processing operations are not included as part of the ToE? And is this satisfactorily justified?

    - *Example: A ToE describing in sufficient detail the processing operation of a web based service such as including the registration of users, the provision of service, invoicing, logging of IP-addresses, interfaces to users and to third parties and excluding server hosting (yet including processing and TOM agreements).*

g. Do the criteria guarantee that the (individual) ToEs are understandable to its audience, including data subjects where relevant?

3 GENERAL REQUIREMENTS

a. Are all relevant terms used in the criteria catalogue (i.e. the full set of certification criteria) identified, explained and described?

b. Are all normative references identified?

c. Do the criteria include the definition of data protection responsibilities, procedures and processing covered by the scope of the certification mechanism?

4 PROCESSING OPERATION, ARTICLE 42(1)

With respect to the scope of the certification mechanism (general or specific), are all relevant components of the processing operations (data, systems, and processes) addressed by the criteria?

a. Do criteria require identification of the valid legal bases of processing with respect to the ToE?

b. With respect to the ToE, do the criteria recognize the relevant phases of processing and the whole life-cycle of data including the deletion and or anonymisation?

c. With respect to the ToE, do the criteria require data portability?

d. With respect to the ToE, do the criteria allow identifying and reflecting special types of processing operations, e.g. automated decision making, profiling?

e. With respect to the ToE, do the criteria allow identifying special categories of data?

f. Do the criteria allow and require assessing the risk of the individual processing operations and the protection needs for the rights and freedoms of data subjects?

g. Do the criteria allow and require adequate account of the risks to the rights and freedoms of natural persons?

…

5 LAWFULNESS OF PROCESSING

a. Do the criteria require checking the lawfulness of processing for individual processing operations with respect to purpose and necessity of processing?

b. Do the criteria require checking all the requirements of a legal basis for individual processing operations?

6 PRINCIPLES, ARTICLE 5

a. Do the criteria adequately address all data protection principles pursuant to Article 5?

b. Do the criteria require demonstration of data minimisation for the individual ToE?

…

7 GENERAL OBLIGATIONS OF CONTROLLERS AND PROCESSORS

a. Do the criteria require proof of contractual agreements between processors and controllers?

b. Are controller processor agreements subject to evaluation?

c. Do the criteria reflect the obligations of the controller pursuant to Chapter IV?

d. Do the criteria require proof of review and updating of technical and organisational measures implemented by the controller pursuant to Article 24(1)?

e. Do the criteria check that the organisation has assessed if a Data Protection Officer (DPO) should be appointed as required by Article 37? Where relevant does the DPO meet the requirements under Articles 37 to 39?

f. Do the criteria check that records of processing of activities are required in accordance with Article 30(5) and appropriately address Article 30 requirements?

8 RIGHTS OF THE DATA SUBJECTS

a. Do the criteria adequately address data subject's right to information and require respective measures to be put in place?

b. Do the criteria require that data subjects are granted adequate or even greater access and control of their data including data portability?

c. Do criteria require measures put in place providing for the possibility to intervene in the processing operation in order to guarantee data subjects' rights and allow corrections, erasure or restrictions?

…

9 RISKS FOR THE RIGHTS AND FREEDOMS OF NATURAL PERSONS

a. Do the criteria allow and require assessing the risk to the rights and freedoms of natural persons?

b. Do the criteria provide or require a recognized risk assessment methodology? If appropriate, is it commensurate?

c. Do the criteria allow and require assessing the impact of the envisaged processing operations for the rights and freedoms of natural persons?

d. Do the criteria, require prior consultation concerning the remaining risks that could not be mitigated, based on the results of the Data Protection Impact Assessment (DPIA)?

10 TECHNICAL AND ORGANISATIONAL MEASURES GUARANTEEING PROTECTION

a. Do criteria require the application of technical and organisational measures providing for confidentiality of processing operations?

b. Do criteria require the application of technical and organisational measures providing for integrity of processing operations?

c. Do criteria require the application of technical and organisational measures providing for availability of processing operations?

d. Do criteria require the application of measures providing for transparency of processing operations with respect to

e. Accountability?

f. Data subjects rights?

g. Assessment of individual processing operations, e.g. for algorithmic transparency?

h. Do criteria require the application of technical and organisational measures guaranteeing data subjects' rights, e.g. the ability to provide information, or to data portability?

i. Do criteria require the application of technical and organisational measures providing for the ability to intervene into the processing operation in order to guarantee data subjects right and allow corrections, erasure or restrictions?

j. Do criteria require the application of measures providing for the ability to intervene into the processing operation in order to patch or check the system or the process?

k. Do criteria require the application of technical and organisational measures to ensure data minimisation, for example, unlinking or separation of the data from the data subject, anonymisation or pseudonymisation or isolation of data systems?

l. Do criteria require technical measures to implement data protection by default?

m. Do criteria require technical and organisational measures implementing data protection by design, e.g. a data protection management system to demonstrate, inform, control and enforce data protection requirements?

n. Do criteria require technical and organisational measures implementing appropriate periodic training and education for the personnel having permanent or regular access to personal data?

o. Do criteria require reviewing measures?

p. Do criteria require self-assessment/ internal audit?

q. Do criteria require measure to ensure that personal data breach notification duties are carried out in due time and scope?

r. Do criteria require incident management procedures to be in place and verified?

s. Do criteria require monitoring of evolving privacy and technology issues and updating of the scheme as required?

…

11 OTHER SPECIAL DATA PROTECTION FRIENDLY FEATURES

a. Do the criteria require the implementation of data protection enhancing techniques? This could include criteria that require enhanced data protection by eliminating or reducing personal data and/or the data protection risk.

- *Example: Criteria requiring enhanced unlinkability by using user-centric identity management such as attribute –based credentials (ABC) over organisation-centric identity management would reflect a data protection enhancing technique.*

b. Do the criteria require the implementation of enhanced data subjects controls to facilitate self-determination and choice?

…

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

Criteria will be addressed in forthcoming guidelines on Article 42(2).

13 ADDITIONAL CRITERIA FOR A EUROPEAN DATA PROTECTION SEAL

a. Do the criteria envisage covering all Member States?

b. Are the criteria able to take into account Member State data protection law or scenarios?

c. Do the criteria require an evaluation of the individual ToE with respect to sector specific Member State data protection law?

d. Do the criteria require the controller or processor to provide information to data subjects and interested parties in the languages of Member States

e. On the processing/ToE?

f. Documentation of the processing/ToE?

g. The results of the evaluation?

…

14 OVERALL EVALUATION OF CRITERIA

a. Do the criteria fully cover the scope of the certification mechanism (i.e. comprehensive criteria) to provide sufficient guarantees so that the certification can be trusted?

- *Example: If the scope of the certification mechanism focuses on health processing operations, a high level of data protection should be guaranteed by defining criteria that ensure, for instance, an in-depth assessment and the application of privacy-by-design and privacy-by-default principles.*

b. Are the criteria commensurate with the size of the processing operation being addressed by the scope of the certification mechanism, the sensitivity of information and the risk of processing?

c. Are the criteria likely to improve data protection compliance of controllers and processors?

d. Will data subjects benefit in respect of their information rights, including explaining desired outcomes to data subjects?