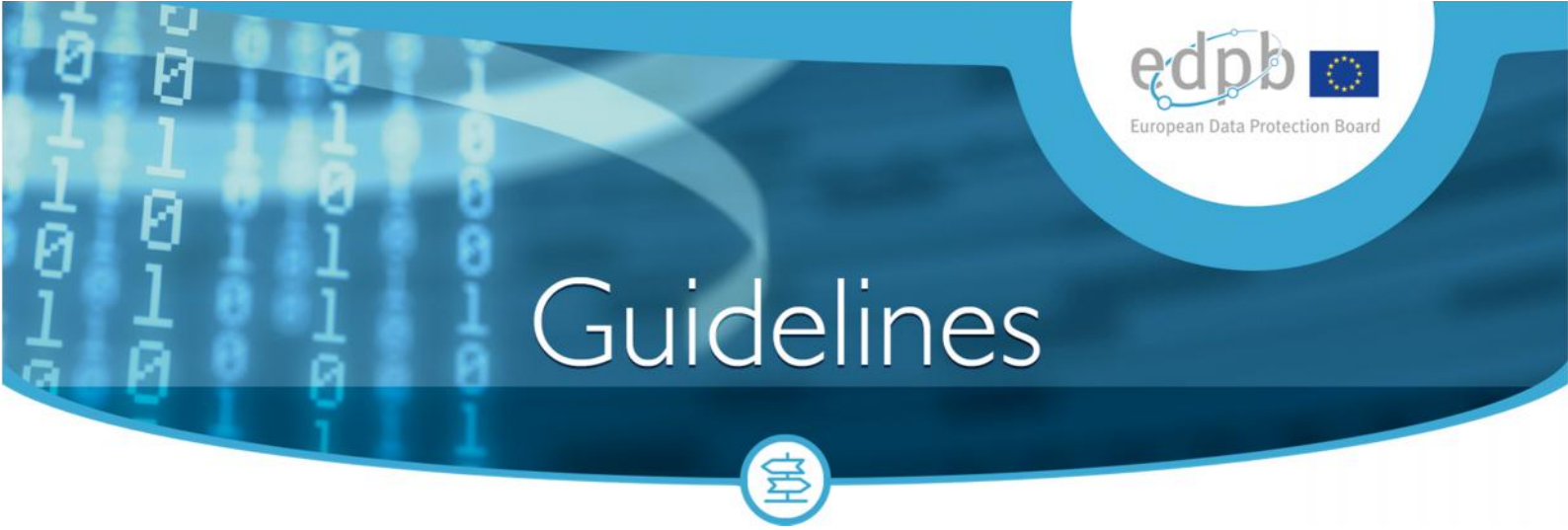

Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation 2016/679 - version for public consultation

Adopted on 25 May 2018

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,

HAS ADOPTED FOLLOWING GUIDELINES:

1. Introduction

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.

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.

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.

Certification mechanisms[3] can improve transparency for individuals, 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 individuals to assess the level of data protection of relevant products and services.[4]

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.

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

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 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.

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.

[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).

The advice contained in the guidelines will be relevant for:

- competent supervisory authorities and the European Data Protection Board ('the EDPB') when approving certification criteria under Article 42(5) and Article 58(3)(f);
- certification bodies when drafting and revising certification criteria prior to submission to the competent supervisory authority for approval as per Article 42(5);
- 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.

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

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".[6]

The GDPR specifies the context in which approved certification mechanisms may be used as an element *to demonstrate compliance* with specific 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);

[6] Article 42(2) further states that certification mechanisms can be established for the purpose of demonstrating the existence of appropriate safeguards for personal data transfers to third countries and international organisations – this will be addressed in separate guidelines.

- sufficient guarantees (processor to controller) as referred to in paragraphs 1 and (sub-processor to processor) 4 of Article 28(5).

Since certification does not prove compliance in and of itself but rather forms an element that can be used to demonstrate compliance,[7] 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 which provide the reasons for granting 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

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"

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).[8] 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".

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).

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

The GDPR does not define "certification mechanisms, seals or marks" – and uses the terms collectively. A certificate is a statement of conformity.[9] A seal or mark can be used to signify the successful completion of a 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 and conforms to specified requirements, stated in normative

[7] See Article 29 Working Party Opinion 3/2010 on the principle of accountability (WP173) highlighted that certification mechanism "would contribute to prove that a data controller has fulfilled the provision; hence, that it has defined and implemented appropriate measures. A data controller or processor may have been awarded certificates for a specific processing operation and yet find itself infringing the Regulation.
[8] International Standards Organisation (ISO) see https://www.iso.org/conformity-assessment.html
[9] See ISO 17000, to which 17065 refers https://www.iso.org/obp/ui/#iso:std:iso-iec:17000:ed-1:v1:en.

documents such as regulations, standards or technical specifications.[10] 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. Certification 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.

2. The role of the supervisory authorities

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.[11] 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;
- encourage the market to develop certification mechanisms.

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

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 to avoid any potential conflicts of interest.

[10] See similarly, Regulation 765/2008/EC, Article 2(20) of the CE marking and ISO 17000:2004, section 3.1 and ISO 17065:2012, section 3.8

[11] See Article 42(5) in conjunction with article 43 and Article 58.3(f), as well as the absence of a task relating to this function in Article 57.

When acting as a certification body a supervisory authority will generally 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 has issued 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, and review including access to information and/or premises, documentation and publication of reports and results, and investigation of complaints. Further, it is reasonable to follow the requirements and criteria as set forward 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

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

- to communicate to the Board the draft decision when it aims to approve the criteria for certification pursuant to 43(3), 64(1)(c);
- to approve of the criteria for certification (Article 58(3)(f)) before accreditation and certification can take place (Article 42(5), 43(2)(b)); and
- to order a certification body (a) not to issue certification or (b) to withdraw certification where the requirements for certification are not or no longer met (Article 58(2)(h).

The GPDR tasks the supervisory authority with approving criteria but not with developing criteria. In order to approve 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 EDPB will provide guidance to ensure a harmonized approach when assessing criteria for the purpose of approval.[12]

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

[12] Guidance will be made available at a later stage in an annex to these guidelines.

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), 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

A certification bodies' 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[13] to determine and set up certification procedures, including procedures for monitoring, reviewing, handling complaints, and withdrawal as well as to present for the purpose of accreditation certification criteria to determine the rules (procedures) under which certifications, seals, or marks are issued (Article 43(2)(c)).

The existence of a certification mechanism and certification criteria are necessary for the certification body to achieve accreditation under Article 43. Yet, a major impact on what a certification body does specifically arises from the scope and type of certification criteria which have impact on the certification procedures and vice versa. Specific criteria may for example require specific methods of evaluation (e.g., on-site inspections, code review). These procedures are mandatory for accreditation and are further explained in the guidelines on accreditation.[14]

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

4. The approval of certification criteria

The certification criteria form an integral part of any certification mechanism. Consequently, the GDPR requires the approval of certification criteria by the competent supervisory authority (Article 42(5) and 43(2)(b)).

[13] A scheme owner creates criteria and procedures but does not carry out certification.
[14] See Article 29 Working Party Draft Guidelines on Accreditation, adopted on 6 February 2018 (WP 261).

The EDPB recognizes the following purposes of approval for 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.

Approval is granted on the basis that 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. Time of approval

Certification criteria must be approved by the competent supervisory authority prior or during the accreditation process. Approval is also required for updated and further schemes or sets of criteria under ISO 17065 prior to their application in certification mechanisms (Article 42(5), 43(2)(b)).

4.2. The competent supervisory authority

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. Alternatively, a certification body can also issue certification in accordance with criteria approved by the EDPB, which may result in a European Data Protection Seal.

4.3. The 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*.

The application for approval of the EDPB should state the intention of the candidate certification body to offer the criteria in a certification mechanism addressing controllers and processors in several Member States.

Based on Article 42(5) the mechanism for a European Data Protection Seal as well as its criteria needs to take into account national sector specific regulations where applicable, e. g., for data processing in public schools[15] and shall envisage a European-wide application.

Requirements for 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;
- description of the certification mechanism specifying;
    - the certification agreements, recognizing pan-European requirements;
    - the language of the reports addressing all affected supervisory authorities.

If certification criteria have been approved by the Board pursuant to Article 42(5), accredited certification bodies may conduct certification under these criteria on Union level. The criteria under such a pan-European certification mechanism may cover data processing operations carried out across Member States.

5. The development of certification criteria

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.

The development of certification criteria should not only consider market demand, but for successful approval, also verifiability, significance, and suitability of certification criteria to demonstrate compliance with the Regulation must be taken into account. The certification criteria should be formulated in such a way that they are clear and comprehensible and that they allow practical application.

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;

[15] The GDPR provides for opening clauses. Member States may maintain or introduce more specific provisions to adapt the application of the rules of the GDPR with regard to the processing for compliance with specified requirements or specific processing situations.

- 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 Articles 32.

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?

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).

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).

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.[16]

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.

[16] It should be borne in mind that processing operations do not coincide with the use of a particular type of technology or programme.

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 natural persons, such as data protection officers for example. Art. 43(1)(b) refers to ISO 17065 which provides for the accreditation of certification bodies assessing the conformity of products, services and processes.[17] 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.

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).

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 concerned individuals.

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

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.[18] 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

[17] See EN-ISO/IEC 17065/2012 Conformity assessment – Requirements for bodies certifying products, processes and services.

[18] See also Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, April 2017, Version 3.1, Revision 5.

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[19] 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 or consumer.

[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
   Whereas 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 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. Processing operations 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.

[19] Also called target of evaluation, ToE, cf. e.g., Common Criteria.

[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.

5.3. Evaluation methods and methodology of assessment

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 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 testing methods and findings collected e.g. during on site audits or from documentation,
- evaluation methods focussing 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.

The level of evaluation has an impact on the significance of the certification. By reducing the level of evaluation to reduce the costs or for pragmatic purposes the significance of a data protection certification will be diminished. Decisions on the granularity of the evaluation on the other hand, a certification may surpass 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.

5.4. Documentation of assessment

Certification documentation should be complete and comprehensive as 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. Thereafter evaluation will allow comparison of the certification documentation with the actual status on-site and against the certification criteria.

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

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."*

To enhance transparency the documentation and communication of results play an important role. Certification mechanisms directed towards the data subjects should provide easily accessible, intelligible and meaningful information about the certified processing operation(s). This information should include at least the

- description of the target of evaluation (ToE);
- the criteria applied to the specific ToE;[20]
- the methodology for the evaluation of the criteria (on-site evaluation, documentation, etc.); and
- the duration of the validity of the certificate.

[20] See section 5.

6. Guidance for defining certification criteria

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. The guidelines for defining certification criteria will 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.

A small local company, such as a retailer, will carry out less complex processing operations. While the requirements for the legitimacy 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 criteria that are, scalable according to the processing activity in question.

6.1. Existing standards

Certification bodies will need to consider how specific criteria take existing relevant 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

Certification criteria must adhere to the declaration (message or claim) of a certification mechanism or scheme and adhere to the expectations it raises. The name also identifies the scope of application and consequently the determination of criteria.

> [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.
>
> [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.
>
> [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.

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 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 in this respect 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

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: 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.