Guidance – Addendum

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

Certification criteria assessment

Adopted on 06 April 2021

Table of contents

1 INTRODUCTION

1. This guidance should be read in line with the EDPB Guidelines 1/2018 on certification and identifying certification criteria according to Articles 42 and 43 of the Regulation and Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation (2016/679). The aim of this additional guidance is to refine elements from EDPB Guidelines 1/2018 for helping:

    - stakeholders involved in the drafting of certification criteria in the context of GDPR certification and;
    - Supervisory Authorities (SAs) and the European Data Protection Board (EDPB) to be able to provide consistent evaluations in the context of certification criteria approval (for both national schemes and EU data protection seals).

2. The recommendations contained in this document must not be seen as exhaustive. The assessment of certification criteria will be carried out on a case-by-case basis, and specific certification mechanisms may require additional measures not covered by this guidance.

2 DEFINITION OF TERMS

3. "General certification scheme": a certification scheme that targets a large range of different processing operations performed by a data controller/processor from various sectors of activity;

4. "Specific certification scheme": a certification scheme that targets specific processing operations performed by a data controller/processor (e.g.: pseudonimyzation of personal data, human resources processing) and / or for a specific sector of activity (example: data processing in stores);

5. "Objective": a target, goal or purpose to be achieved by a criteria or a set of criteria;

6. "Certification guidance" – assistance for auditors or implementers related to how criteria could be met under differing circumstances, scale or context.

3 SUBMITTING A CERTIFICATION SCHEME TO A SA

7. In order to facilitate the process of criteria approval by SAs and the EPDB, SAs may require scheme owners to engage early with them. This allows for an informal discussion on the scope of the certification mechanism and on the intention of the scheme owner. This allows SAs to prepare, assign and allocate resources as needed, and possibly, where applicable, to communicate with the local NAB. Depending on the agreements mentioned above between SAs and NABs, there may also be a working protocol in place between these bodies to facilitate applications for approval that has to be followed by scheme owners.

8. At an early stage of the drafting process, scheme owners should consider:

    - What is the market demand for this certification mechanism?

- What will be the benefits of this certification mechanism for the data subjects, for data controllers and processors?

9. Going into more detail based on the answers to these questions, additional considerations would be:

   - What types of organization will ask for a certification? E.g.: is the scheme aimed at a specific sector, or at a specific type of organization like associations or SMEs?
   - What type of processing operations will be certified under the scheme? E.g. is the scheme aimed at a specific type of activities / processing operations, like the processing of medical records, or the use of a specific technology, like cloud computing services?
   - In which EU Member State(s) the certification mechanism is intended to be used or is it intended to be used in all EU Member states, as an EU data protection seal.

10. The scheme owner's decisions on these topics is to be reflected in the scheme and the criteria. For instance:

    - A scheme that is aimed at a specific sector will take into account sectoral law. The audit approach laid out by the scheme will be expected to address commonly found risks in the sector.
    - A scheme that is aimed at the use of a specific technology will contain criteria that are specific to that particular type of technology (e.g. regarding anonymization or encryption techniques).
    - If a scheme is to be used in more than one member state, the scheme owner will be able to demonstrate that their certification processes will take on board all relevant national regulations in those member states.
    - If a scheme aim at handling different sectors, technology and/or categories of processing (general certification scheme) the same expectations will apply.

    The informal engagement of the scheme owners with the competent SA will help to clarify these expectations.

11. If applicable, at the conclusion of an informal phase, it is likely that SAs will expect that scheme owners will make applications formally when they have good grounding to do so and where schemes are in a mature state of preparation.

12. With this in mind, it is advisable that scheme owners should be prepared to provide to an SA:

    - Details of scheme owner identity including contact details, establishment and data controller status, including, where applicable, the location of the headquarters and organisation establishments that intend to make certification decisions.
    - Where already known, the name of certification scheme stakeholders (e.g. where a scheme owner will license the scheme to CBs in member states, if applicable logos/graphics/seals that are used to represent the certification)
    - Where the scheme owner is a CB any relevant references for existing ISO 17065 accreditation with local or other NABs.
    - The name of the certification scheme and a description of the scope of the certification scheme, including the GDPR target area(s) of compliance and to the extent possible, the intended ToE.

- The specific processing operations covered by the certification scheme (accounting for the certification scheme being general or specific)
- The member state(s) the certification mechanism is intended to be operated in, and if the scheme is expected to be national, multi-national, or an EU Seal
- The organisations or sectors that are the target audience and the market demand that exists for this certification scheme.
- An overview of the scheme criteria and how the criteria and objectives are intended to improve data protection compliance of controllers and processors and how data subjects will benefit in respect of their information rights, including explaining desired outcomes to data subjects.
- The type of personal data the certification scheme applies to, including special categories of data, location data, financial data.
- In addition, scheme owners should be prepared to confirm to an SA :
    - that EDPB guidelines are taken into account and in particular that the criteria address all the sections required by Annex 2 of the EDPB certification guidelines
    - to show that the criteria describe how the ToE should be defined by controller or processor
    - that the certification mechanism takes into account for the requirements set out in ISO 17065/2012.
    - and to enumerate any international, European or national recognized and relevant standard (e.g. ISO, CEN/CENELEC, etc…) that are included or referenced and provide the basis for the certification scheme.

4 CERTIFICATION OF PRODUCTS / SERVICES

13. The EDPB Guidelines 1/2018 on certification state that "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."

14. Controllers or processors can apply for certification for the processing activities they undertake that make use of personal data. Consequently, standalone products cannot be GDPR certified. In this case no data controller / processor is yet involved in an actual and ongoing activity. So, no personal data is currently being processed. If and when a data controller/processor makes use of such a product in the context of a processing operation, it may become an element of the GDPR certification of a product, process or service. Nonetheless, GDPR recalls[1] that technology and software providers are "encouraged to take into account the right to data protection when developing and designing such products, services and applications and, with due regard to the state of the art, to make sure that controllers and processors are able to fulfil their data protection obligations. "

15. As such, a software provider cannot apply for certification for a software tool if it is a standalone product used only at the client's site without the involvement of the provider with regard to the client's processing of personal data. This is because GDPR certification is intended for controllers or processors

[1] See GDPR recital 78

and not for manufacturers of standalone products. However, if the same software includes for example a data storage service involving the provider in the processing of personal data, the provider can apply for certification for this part (because the provider is likely to be a personal data processor). In that case, it shall be clear where the processing activities performed by the end user stop and where the provider starts performing them when defining the scope of the certification, but this too is required in order to clearly delineate controller and processor relationships and responsibilities under GDPR.

16. In this context, we can identify two kind of cases:

    1) the certification applicant is not the software provider/developer/manufacturer: the ToE will cover some of the data processing resulting from the use of the software by certain controllers/processors (example: the HR process of a data controller that make use of an HR software can be certified).

    2) the certification applicant is the software provider/developer/manufacturer: the ToE can cover some of the data processing that are provided "as a service" with the software by the owner as a controller/processor (example: the data storage function of an HR software).

17. In any case, the scope of the certification (what can be certified?) and the ToE (what is certified for a specific controller / processor i.e the object of certification) need to be defined and will be provided on the certificate for transparency. For instance, the owner of a HR SaaS will not be allowed to claim that the usage of its software for HR processing has been certified if the scope of its certification is only the data storage service that the HR SaaS provides[2].

5 SCOPE OF CERTIFICATION AND TARGET OF EVALUATION

5.1 Evaluating the Scope of a Certification Scheme

18. All certification schemes shall have a clearly defined scope and also indicate what is not included – to avoid "scope creep". This should be the central basis for the assessment at supervisory authorities and at EDPB level (if the schemes claims to be applicable for any kind of processing, it will be challenged on how the scheme can be applied to any kind of processing in a consistent and reliable manner, including where special categories of data are processed).

19. This also plays an important role in the subsequent communication to the relevant public who need to understand what is certified and what is not. This should give a clear understanding of what this concretely means for them, their personal data and how GDPR obligations will be undertaken and delivered.

20. The scope and objectives of a GDPR certification and the supporting processes have to take into account not only the certification approach but also the related regulatory aspects that include the precise links to GDPR requirements and, if applicable, national obligations.[3] A certification scheme

[2] Attention should also be paid to the fact that conformity marks should not be used in such a way as to create a false impression of the purpose of the certification or to mislead consumers.

[3] Certification under GDPR articles 42 and 43 opens the possibilities for the different stakeholders to be innovative. EDPB and SAs should support this possibility and contribute to it.

should be developed to address the GDPR requirements while ensuring an alignment and conformity of the certification scheme with any included or leveraged ISO standards and certification practices. As a result, a scheme should add value to an organization by helping to implement standardized and specified organizational and technical measures that demonstrably facilitate and enhance processing operation compliance. This reflects what EDPB Guidance 01/2018 means when is says the purpose of criteria approval is " 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. ".

21. A scheme scope needs to be defined in some way to be practical, tractable and to be able to provide an added value. General certification schemes might be applicable to multiple sectors and/or to many kinds of processing activities etc. but, at the same time, they need to be limited to be manageable. For example:

- by restricting their application only to specific or clearly defined and delimited processing activities within the scope and objectives of the scheme that are considered low to medium risk (in this case, a clear risk assessment method needs to be included in the scheme to select and define the ToE and restrict it to low and medium risk[4]);
- by excluding some topics that are not meaningful within the context of the certification scope (in any case, this option is only possible if the topic isn't expected to be part of the scope and that the scope isn't senseless without the topic);
- by focusing on the GDPR articles that are relevant to the scope, and not including articles that are irrelevant within the context. For instance, a scheme that focuses on security of processing does not need to cover GDPR articles that are irrelevant to that particular scope[5]:
    - in order to facilitate the assessment of certification schemes, scheme owners should provide detailed explanations regarding their scope and indicate what exactly is evaluated (e.g. the added value the scheme brings). They should explain in how far the scheme delivers what it promises: a clear countable expectation should be formulated. This explanation should not just state that the scheme covers "cloud computing" as this is too general;
    - to ease understand of what is expected as a demonstration of conformity with certification criteria, a scheme shall not claim something that is not clear enough to be assessed.

22. For example, the scope of a certification mechanism related to cloud computing could be SaaS, IaaS and PaaS. Additionally, SaaS can be further divided in sub-categories because providing storage capacities is very different from providing other services (e.g. support for software upgrades). A company might also decide to certify only of one of its service offerings, or even a part of a particular service in certain circumstances. The scheme owner should ensure this is clear and allow for a suitable ToE that reflects the scope to be determined. In this cloud computing example the target of evaluation could go to a level of detail, like for instance: "Data storage service provided by MySaaSDataStorage".

[4] It doesn't exclude the potential requirement of a risk assessment method in other cases

[5] As a certification can be perceived as an indication of compliance with the GDPR, such restrictions need to be transparent and clearly identified in order to avoid misleading data subjects.

23. “Transparency is a key element”.

The scheme or the supporting documentation should make clear its scope to organizations who will seek to be certified, and in so doing define what kind or sector of organization may make use of the scheme. For instance, a scheme that sets out standards for compliant record keeping for any industry or sector with any kind of data processing activities may not be able to encompass all purposes and contexts of such processing in order that demonstrable compliance can be certified in all cases. In this instance, the scheme needs to clearly specify how this is possible, or the scheme owner should reconsider the scope of the scheme by reducing its generality. It is essential that a certification scheme is clearly structured and comprehensible, which ensures transparency towards any interested party (including data subjects) so that anyone dealing with the scheme can understand the process and criteria of a certification. Where a scheme is assessing only part of the GDPR requirements, such limitations, if admissible at all, should be clearly communicated to the data subjects to prevent misinterpretation.

24. “The importance of supporting processes”

Certification schemes need to define the implementation of supporting processes in order to ensure that all relevant situations are covered and that certification conclusions of different certification bodies (CBs) remain coherent during assessment of processing operations. This supporting system is especially important for general certification schemes, meaning that even more effort is involved in defining scheme criteria and the supporting processes to ensure that their applicability to diverse categories of data processing activities does not affect the consistency and uniformity of the certifications issued according to the same schemes. As CBs are accredited to certify against specific certification schemes, it is of utmost importance for them to implement accordingly the supporting processes related to each certification scheme.

5.2 Evaluating the Procedure to Determine a Target of Evaluation (ToE)

25. Before performing any evaluation activities, the CB, working with the applicant (the data controller/processor) identifies and specifies the ToE. This should encompass the systematic identification and description of the data processing activities, including:

- a detailed description of the data processing activities and a comprehensive illustration of the processing modalities in the ToE, including a clear indication of where the processing in the ToE starts and where it ends. It may also include all data flows, access points and interfaces, reporting, data transformation or export, data set combinations or merges. It should do so in the form of a diagram or a drawing, including any external data flows, query or programming interfaces, aggregations, etc;
- a justification of any exclusions of interdependent data processing operations / activities from the ToE. If this case occurs, it must be ensured that the coherence of the ToE is not undermined;
- the identification (e.g. location, origin) and description of the data or data types processed and in particular the personal data involved;

26. In the certification scheme the requirement for a detailed description of the concrete ToE is to be made and corresponding requirements for the consistent application of certain accompanying processes are necessary in order to enable a consistent application of the certification criteria in comparable cases. Following the requirement 7.3.1 from ISO 17065, a certification scheme shall require a Certification

Body to refuse any ToE that is ambiguous or misleading, or risks to be misinterpreted by data subjects or by other third parties, or if the ToE is itself not compatible with the scope of the certification. A Certification Body may decide to adapt the target of evaluation (based on a procedure that requires to document the change) during the course of the certification process.

ToE transparency on the certificate

27. Considering the item 7.7.1(d) of ISO 17065, the certification body should provide a clear description of the ToE on the certificate. Even if a summary of a certification report is accessible to data subjects or other parties, it is important for any party to be able to quickly identify and understand which process(es) are actually covered by the certification. Therefore a certification scheme should contain clear and precise requirements as to the content describing the ToE that will be set out on certificates.

28. If the number of processing activities is large, this might be confusing for data subjects. Therefore, in this case, the certificate can contain an executive summary of the certification and provide a link to an external document containing the details of the certified processing.

Content on the certificates needs to be transparent and clear for data subjects and other concerned stakeholders.

6 CERTIFICATION CRITERIA

29. ***How specific do certification criteria need to be? Paragraph 31 of EDPB Guidelines 1/2018 on certification indicates that certification criteria, in order to qualify for approval, need to contribute to the consistent application of the GDPR. How much level of detail in the certification criteria and/or guidance for the auditor is needed in order to achieve this?***

30. Certification is not about stating an entity is 100% GDPR compliant. But certification aims to show concerning a particular TOE and its processing operation(s) that the applicant made everything possible, to satisfy certification criteria[6].

31. Certification criteria need to be framed in such a way that:

- they are consistent with the relevant stated objectives;
- an evaluator can assess the processing objectively and to defined levels of implementation;
- an evaluator can determine if those criteria levels are met or not, ensuring consistent and repeatable evaluations of the same criteria;
- the risk of subjective or diverging interpretations of the criteria is minimized;
- the criteria are applicable to diverse contexts (sectorial context, technological context), including their scalability to meet the requirements of SMEs.

32. A certification scheme should therefore also be clear about:

[6] GDPR Article 24(3) : « *Adherence to approved codes of conduct as referred to in Article 40 or approved certification mechanisms as referred to in Article 42 may be used as an element by which to demonstrate compliance with the obligations of the controller*.

- the nature of the evidence required by the evaluator is consistent: for instance, it would not be acceptable that one CB requests actual proof or on-site inspections whereas other CBs assessments of the same topic are just paper-based;
- what needs to be demonstrated (what is the purpose of the criteria).

33. The current EDPB guidelines 1/2018 on certification include guidance for defining certification criteria in paragraph 67 as well as objectives and implementation guidance for the auditor to be included in a scheme.

34. "Certification criteria should be uniform": another important point is the question of whether the criteria contain sufficient content to allow for a coherent and consistent application of the same certification scheme within a CB (in relation to different certifications / applicant) or between different CBs. This is more challenging for general certification schemes and for this reason those schemes need to put a special emphasis on clarity of scope and purpose from the beginning about their scope and purpose. Certification criteria should not be left open to interpretation by one or by different CBs otherwise there is a risk that the evaluation methodology and the measures of compliance used will differ, even if they still lead to the same certifications. In order to mitigate this risk, a guidance note to auditors can play a key role.

35. "Certification criteria should be relevant to the targeted audience": certification should be meaningful when applied and assessed in the context of a ToE (taking into account the targeted audience), so the criteria should be realistic and proportionate to the scheme's scope and its expected ToEs. The certification scheme may envisage differentiated criteria taking into account other elements such as the context, scope, objectives and purpose of the validation of criteria. Those elements need to be evaluated at the very beginning of the criteria assessment in order to check how they make sense, are realistic and relevant to the ToE.

36. "Certification criteria should be 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" and "be flexible and scalable for application to different types and sizes of organizations"

37. In addition, criteria can be generic (low level of detail) or more specific (high level of detail). However, a criterion is different from its related objective because the former should be explicit about what is expected as an output/evidence. As an example, "Privacy by design shall be implemented" can't fulfill the properties of a criterion (uniform, verifiable and auditable) but it could be set as an objective. In that case, an example of criteria could be "when developing software, test data sets are to be composed of anonymized data or dummy data. Anonymization requires [conditions to be met]. Only if [conditions to be met] pseudonymized data is allowed to be used. Pseudonymization requires [conditions to be met]. If pseudonymization is to be used, [conditions to be met]".

38. The following points may assist when drafting and assessing certification criteria:

    1. An individual criterion always needs to be assessed taking into account its targeted context. Understanding how the ToE is to be selected and defined (as defined in the certification scheme) will likely need to be taken account of in order to perform this assessment. Does this criterion need to be assessed together with other criteria in order to have a complete "coverage" of a topic? Are there relationships and dependencies among criteria?
    2. In view of that, it should be clear what the objective of the criterion is in the context of the certification scheme's scope itself. Why is it relevant? What should be the expected outcome/result? What is the objective for an evaluator in assessing a criterion (example: is it

to check for "well formed" records or to look at the process that leads to those records and to their content?).

3. Then, based on that, it should be assessed whether the requirements in the criterion are sufficiently detailed to allow the conclusion that the expected outcome/result is met during an evaluation. In addition, it should be considered if the necessary (formal) evidence for the auditor is required to be able to draw the right conclusions (ex: policies & procedures, formal allocation of responsibilities, trainings and awareness programmes, technical standards, etc.)? If not, why not – what added value is provided above a mere repetition of GDPR (the scheme owner should provide an explanation)?
4. The criteria should also cover all possible scenarios that can reasonably be expected in the context of the scheme's scope or where applicable, it can be covered in a notice for auditors. In the latter, a particular attention has to be taken to ensure consistent certification amongst applicants. This is especially true in a general certification scheme where TOE may be very different.
5. It cannot be excluded that there will be cases, where a criterion has been followed to the letter, even while the evaluators are not persuaded that the result is GDPR compliant (for example due to a different interpretation of the law / criteria etc.). Such a situation could lead to a non-conformity of the criterion in the long term. The auditor should write down this finding in the audit report and describe the "improvement" actions. By doing so, the auditors (and the CB) are performing their task in an accountable way and the data processor/controller cannot claim it was not informed.

39. "verifiable, auditable and relevant" :

The current EDPB Guidelines 1/2018 says criteria should be verifiable, auditable and relevant. At the same time and as set out above, the same certification criteria may need to be assessed differently depending on the TOE or if, for instance, special categories of personal data are used. Such flexibility needs to be clearly defined in the criteria or this flexibility[7] needs to be handled in adding criteria that apply only, for example, to these special category data.

40. If we are to, for example, certify an "effective pseudonymization process" one element of evaluation may be to do with security of the algorithm chosen for encryption or hashing. A good criterion for a certification scheme focused on pseudonymization might specify details such as: what encryption or hashing scheme to use, how many rotations would be chosen, what testing would need to be evidenced with representative data, what sampling checks happen when it is used "live", how the state of the art is monitored, how the evaluator can check the data controller is actually using it (Code, configuration etc). Each of these elements would have to be evaluated and confirmed as being satisfied in order to reach the certification schemes thresholds. A different or competing scheme for the same question may have different criteria or "pass levels" that have to be met. For instance, if the scheme targets specifically pseudonymization process, a badly defined criterion might say "*A suitable encryption scheme should be used and a record kept of when it has been used*". This leaves the evaluation of "suitable", the record keeping process, and other important assurance elements such as testing (not mentioned) up to interpretation by different CBs, and ultimately inconsistency and possible misapplication. As a result, it may happen that some organisations may be certified when they

[7] Such flexibility may mainly apply to general certification schemes and it should be framed accordingly.

should not be. A scheme that is built around such poorly defined criteria does not result in a good instrument of accountability.

Criteria example

Given the above guidance, the following section provides an example of a reasoned assessment of a sample criterion.

Section: Data Subject Rights	
Section objective: Enabling the effective exercise of the rights of data subjects	
Criteria	**Notice**
The entity shall demonstrate that a procedure or mechanism is in place to effectively implement the request of the right of a data subject to rectify his incomplete or erroneous personal data.	The entity should keep records of the data subject request, the content of the communication with data subjects, the follow-up, and if applicable, the reason for not complying with a data subject request.

- ⇨ This criterion basically corresponds directly to the text of Article 16 of the GDPR. On the contrary, certification criteria must go more into detail as to what the GDPR article demands in order to meet the standards the same criteria wish to demonstrate. This sample criterion is too abstract to achieve this. For instance, does the evaluator assess and determine that the records accurately reflect the actual processing that is occurring or just that the records are "well formed"?

- ⇨ For this specific case, there should be other complementary criteria to this one, which provide more specification of what needs to be implemented. For instance, GDPR article 16 requirements are more demanding than just granting the right of rectification (e.g. requirements of delay, to take into account the purpose of the processing). Other criteria complementing this example might be something that could be accepted. However, the reasons the individual criterion are separated this way by the scheme owner needs to be clear and understood because there may be implications for the auditor and if there is a risk that assessment will be conducted too narrowly when looking at this individual criterion.

- ⇨ There can be additional criteria about for example data integrity. Assessing a criterion requires to take into account the context since there may be many more criteria that will specify the elements linked to this criterion. However, each criterion needs to be autonomously auditable and verifiable, because each non-conformity needs to be raised based by the auditor on one or several specific criteria. Auditors must apply all applicable criteria and systematically report any identified non-conformity. Having a general requirement/statement and then more specific related criteria has to be carefully handled because if a non-conformity cannot be referred to one of the specific criteria it may lead to confusion regarding what exact aspect of the requirements the non-conformity concerns. As a general principle, in case of non-conformity, the criteria should enable the entity to understand what has to be remediated and improved.

- ⇨ By default, criteria are to be demonstrated: there is no need to specify that the entity "shall demonstrate"

⇨ Terms like "effectively" should be avoided, as they can be difficult to assess it in a predictable way. Instead, criteria should define what needs to be measured and what level of measurement is needed to achieve what the auditor is checking.

7 NOTICE TO AUDITORS / ASSESSMENT NOTES

41. Criteria can be supported by a notice to auditors that can clarify how these criteria should be assessed in varying contexts. Such information can include best practices and/or more detailed information / explanations directed towards specific interested parties such as auditors or applicants.

42. A notice for auditors can for example contain more detailed explanations of the criteria or regarding specificities of certain sectors, countries, technologies or size of organization. If a notice is in place it has to help auditors to determine the most adequate approach to check certain measures, it can oblige them to perform certain verifications (e.g. use of a specific sampling method in a specific case, obligation to check the whole population, etc.) or it has to require certain standards with regard to the auditor's documentation of the evaluation activities.

43. Attention should also be paid to the fact that the content of such a notice should not lead to incorrect assessment of conformity with the certification criteria.

Example of a possible approach:

44. The criteria contain the rules to be followed to have an expected result and represent for the auditors the "control objectives". Applicants need to make sure that their internal controls or measures be designed, implemented and operated to allow them to reach these control objectives defined by the certification criteria. When performing their certification audit, auditors will then check whether the design, implementation and operation of these controls or measures at the applicant's organization comply with the control objectives defined by the certification criteria.[8]

45. General guidelines for auditors can for example require that evaluation tasks be structured as follows:

- **Design and implementation**: The auditor will look at the design or description of a control or measure (for example in the form of a procedure) and verify if it will work in theory as required by the certification criteria: The auditor will try to determine if it is designed to comply with the certification criteria. This is an important part in the auditor's work because if an auditor finds major flaws in this step, it is possible and often likely that the control or measure does not work consistently as required by the certification criterion in practice. For example, when a procedure is not correctly documented, or documented for another purpose than the one the criteria is targeted at, the person performing the control might start to improvise and develop their approach or perform their procedure inappropriately from what is expected or required by the criteria.

[8] This is a specific approach, some schemes somehow include a step-by-step recipe when following the criteria (like the Plan-Do-Check-Act of ISO). In that case, the "rules" have to be followed because they are part of the criteria. For instance, this is the HLS structure of ISO which is common to lots of widespread management systems (ISO 9001, 14001, 27001). But there are also other schemes (especially in the service certification domain) where only an output is expected and it may also be suitable for GDPR certification. The criteria do not necessary have to contain such "rules" (although it could very useful to ensure compliance over time).

- **Operating effectiveness**: After having reviewed the design and implementation of a control or measure, the auditor will test the operating effectiveness of this control or measure: He/she will check if the control or measure works in practice as it should or as documented, through – depending on the type of control – observation, walkthrough, sampling, interviews, interaction, e.g. with an interface, etc.

46. This additional information should not:

- refine the certification criteria: an information note may clarify criteria or indicate good practices, but it should not change the criteria otherwise it would become part of the criteria itself. This would also pave the way to subjective interpretations and applications of the criteria. In other words, this information shall not be seen as an extension of the criteria and thus considered as a criterion itself.
- be too detailed about how to implement the criteria. It's up to the applicant to implement measures that fits to his own environment to comply with the criteria.

47. Other considerations:

- The difference between the audit methodology used for the assessment of criteria and the "gap analysis" techniques may be underlined. A gap analysis may consist in checking that a controller or processor has measures to provide for each point of a check list. As a result, the controller or processor may get scores and improvement suggestions based on the state-of-the-art. In the case of certification, as well as a check-list with conditions there will also be a threshold that shall be met for each point of the checklist or criterion. This means that certification is more formal and deterministic than a check list approach. It also does not mean that this "threshold" cannot take into account the context of the processing but this has to be specified by the criterion and also how to handle this context.

8 EU DATA PROTECTION SEALS: NATIONAL LEGISLATIONS COVERAGE

48. As noted in EDPB Guidelines 1/2018, based on Article 42(5), the mechanism for a European Data Protection Seal as well as its criteria needs to be customizable in a way as to take into account national regulations where applicable. This means that, during the approval process, scheme designers or owners must be able to demonstrate to SAs and the EDPB how the scheme will operate consistently and effectively in Member States given a comprehensive review and consideration of local conditions, restrictions, legislation or prerequisites.

49. In addition to requirements listed in the EDPB Guidelines 01/2018 on certification (Section 4.2.2 devoted to European Data Protection Seal criteria), the scheme owner shall also :

- provide an explanation of how the list of applicable national specific regulations was setup;
- provide an explanation of how the list of national specific regulations to be covered is kept up to date, including periodic and transparent reviews (for instance, the list may be confirmed by a legal advisor);
- keep version and date records of the list of national regulations.

50. The methodology proposed to demonstrate the compliance to the criteria in the context of national regulation shall be transparent and repeatable. For general certification schemes, elaborating specific criteria based on applicable national regulations might be highly complex[9].

51. However, there are possible means for scheme owners to manage this requirement. For instance:

- country-specific guidance to assess criteria that are suitable for all Member states may be provided ;
- some criteria may be focused on the application to national regulations, detailing what the data controller or processor needs to demonstrate and how it will be assessed (e.g. identify relevant specificities in national data protection regulations that apply to the data processing of the ToE, define and apply measures to address them, etc);
- the scheme may define a process that involves group of experts that will perform an assessment of the compliance of the data processing in the ToE with the applicable national provisions, at the time the CB intends to operate in a Member State. Such a mechanism should also ensure that these experts are properly qualified and provide consistent and coherent assessments (for instance a network of experts could be included in the scheme certification procedures). The expert group process would need to be transparent and its assessment report would have to be made available for scrutiny, on request, by a supervisory authority or the EDPB.

Role of the Scheme Owner:

52. As said above, the scheme owner is responsible for establishing adequate mechanisms and procedures to address the relevant national obligations related to personal data protection in each Member State where the scheme is operated. For instance, where the scheme owners leverage on network of experts, it shall require the adequate expertise and shall operate with CBs making use of their scheme in a timely fashion, and taking account of each MS provisions.

Role of the EDPB:

53. The EDPB works with the competent SA and the scheme owner on approval of criteria and the mechanism that manages use of the Seal in each MS[10].

Role of the CB:

54. The CB remains accountable for the certification activities it undertakes and for ensuring, with the scheme owner, that its certifications under the scheme account for relevant national provisions. The CB must be accredited as required with relevant member states accreditation body or SA.

Role of the SA:

[9] If the applicable national regulations cannot be easily determined, this may be because the scope of the scheme is not clear or focussed enough.

[10] Approval procedure: Refer to EDPB document on the procedure for the approval of certification criteria by the EDPB resulting in a common certification, the European Data Protection Seal (available on the EDPB website https://edpb.europa.eu/our-work-tools/our-documents/procedure/edpb-document-procedure-approval-certification-criteria-edpb_en)

55. Following EDPB's procedure (informal phase for EU Data Protection Seal adoption)[11] each SA should check the adequacy / compliance with national applicable specific regulations of the proposed mechanism and, the proposed criteria.

56. This is one possible approach. Other means to ensure that EU Seals are "customizable"[12] for use in differing member states are likely to be developed by innovative scheme owners, in conjunction with SAs and the EDPB, over time.

9 CHANGES AFFECTING CERTIFICATION

1) Scheme owners need to have a process in place to manage certification criteria updates. This process needs to be defined as part of the certification scheme[13]. Scheme owners shall envisage a periodical review of their certification schemes.
2) The competent SA is in charge of reviewing updates made to the certification criteria. Therefore, the scheme should ensure that scheme owners communicate certification criteria updates to the competent SA and whether they involve (or not) substantial changes to the certification criteria.
3) The competent SA assesses the certification criteria updates. The competent SA may agree (or not) that the scheme owners' classification of the updates is correct (see below for details). The scheme owner revises the scheme, if necessary.
4) The competent SA follows the EDPB procedure related to national certification criteria or EU data protection seal in order to approve the updates.

57. The certification criteria updates should be classified as "major" and "minor" updates. Certification criteria updates directly impacting on the application of data protection requirements and any modification that would reduce or weaken existing criteria shall be considered by default as major updates. Updates for 'technical' purposes may often be considered as minor updates.

58. Amongst others, the following elements may be included when a scheme owner classifies certification criteria updates:

- Major updates (involving substantial changes of the certification criteria):
  - Recommendations in EDPB guidelines that lead to significant changes for the certification criteria related to the scope of the certification;
  - Court decisions that lead to significant changes for the certification criteria related to the scope of the certification;
  - Adoption of delegated acts of the European Commission in accordance with Articles 43(8) and 43(9) impacting the certification criteria;

[11] See EDPB document on the procedure for the approval of certification criteria by the EDPB resulting in a common certification, the European Data Protection Seal.
[12] See paragraph 40 of EDPB Guidelines 1/2018 on Certification and Identifying Certification Criteria.
[13] Refer to EDPB Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation (2016/679), section 7.10 of Annex 1 for more details about the content of such a procedure.

- Amendments to data protection legislation (EU or national) that lead to significant changes for the application of data protection requirements impacting the certification criteria;
- Adding new criteria covering a new objective;
- Deleting criteria that removes the coverage of an objective;
- Substantially altering existing criteria in any way;
- Change of the scope of a certification scheme;

- Minor updates (not involving substantial changes of the certification criteria):
  - Clarification of language;
  - Corrigendum;
  - Adapting criteria following the return of experience on the assessment of criteria (for example for enhancing consistency amongst certification awarded);
  - Court decisions that lead to minor changes for the certification criteria related to the scope of the certification;
  - recommendations in EDPB guidelines that lead to minor changes for the certification related to the scope of the certification;
  - Amendments to data protection legislation (EU or national) that lead to minor changes for the application of data protection requirements impacting the certification criteria.

59. Any changes to data protection regulations or court decisions related to data protection shall be taken into account without delay by scheme owners. The competent SA needs to be informed by the scheme owners about the criteria updates as fast as possible. The competent SA may in exceptional cases inform scheme owners about the necessity to update certification criteria.

60. Ideally the scheme owners should also provide to the competent SA a yearly report containing an assessment relating to certification criteria updates.

61. Note: As a priority, controllers and processors seeking or those that have already been awarded a GDPR certification, must always ensure their continuous compliance with data protection obligations. At the same time, a granted certification remains valid during possible transition periods (by default until the next surveillance audit) between any change in data protection requirements and the update of the certification criteria to reflect those changes. The change procedures to be agreed by the CB could include: transition periods, approvals process with competent supervisory authority, reassessment of the relevant object of certification and appropriate measures to revoke the certification if the certified processing operation is no longer in compliance with the updated criteria.

10 ACCREDITATION & MULTI-NATIONAL CERTIFICATION

62. Notwithstanding EU NABs' own procedures and recognition and accreditation of CBs[14], the following clarification of the EDPB guidelines 1/18 on certification (paragraph 34, 40 & 44) may be useful where CBs intend to operate in multiple Member States.

[14] See for example sections 3.2.3 and 4.2 of European Accreditation document EA-1/22 at [https://european-accreditation.org/publications/ea-1-22-a/]

General consideration:

63. The examples below discuss various scenario where certification schemes are operated in Member States and across the EU. However, in each scenario, it should be recalled that certification under GDPR can be granted only to controllers or processors for identified processing activities. In order to determine to which entity a certificate can be granted, the usual rules to determine if an entity is controller / processor have to be applied. If during the assessment of a ToE, it is not possible to identify the controller / processor for the processing in scope, the certification can't occur for this processing activity and it must be excluded from the ToE. Organizations can refer to the EDPB "Guidelines 07/2020 on the concepts of controller and processor in the GDPR" to identify their role in relation to the processing if personal data.

10.1 Scenario 1: CB established only in country A wants to certify against a national certification scheme X in countries A, B & C.

	Country A	**Country B**	**Country C**
CB	Accreditation	No accreditation (provided that the CB in country A remains responsible for issuing certifications and managing certification activities of its subsidiaries/offices in country B and C)	No accreditation (provided that the CB in country A remains responsible for issuing certifications and managing certification activities of its subsidiaries/offices in country B and C)
National certification scheme	Adoption of the certification criteria by country A's SA	Adoption of the certification criteria by country B's SA	Adoption of the certification criteria by country C's SA

64. In which country(ies) needs the CB to be accredited?

- If the certification body is only located in country A, it has to be accredited in country A, provided that it operates in countries B and C through subsidiaries/offices which not manage

and perform certifications autonomously (the same logic apply to certification bodies that release an EU DP Seal certification).[15] [16]

- Where a CB has a headquarter in a Member State (MS) and other establishments/offices on the territories of other MS, the accreditation granted by the SA competent for the headquarter is sufficient and there is no need to obtain separate accreditations in other MS by other establishments or offices of the same CB**,** provided that they issue certifications under the control of the main establishment of that CB.
- It also implies that depending on the context of the establishments/offices on several territories of MS, CB may require several accreditation. This situation has to be assessed on a case by case basis taking into account the activities of the CB's establishments/offices (see scenario 2).

65. In which country(ies) have the certification criteria to be adopted?

- The certification criteria have to be adopted by the SAs of countries A, B & C.

66. The SA in country A leads the adoption of the certification criteria under its national initiative. If, taking account of the scheme criteria and applicable specific national regulations countries B & C adopt the certification criteria subsequent to its adoption in country A, countries B & C may adopt the certification criteria X without triggering an EDPB opinion under article 64 of the GDPR and rely on the opinion given to country A, according with the EDPB's rule of procedure art. 10.4 that states that "In accordance with Art 64 (3) GDPR, the Board may decide without undue delay and within a deadline set by the Chair, not to give an opinion under Art 64 (1) and (2) GDPR, because another opinion on the same matter may have already been issued."

67. Potential impact: Depending on the scope of the certification, criteria may have variants in the different countries in order to comply with specific national regulations:

- in order to handle these cases, the certification criteria have to cover the national requirements of countries A, B & C before the lead SA triggers an art. 64 procedure
- to be successful, country A, B & C have to cooperate during the informal review phase for the certification criteria X following the EDPB procedures for adopting certification criteria in the context of a national initiative.

[15] The accreditation system of CBs envisaged by Article 43.1 and 43.3. GDPR is carried out on the basis of requirements of Regulation 765/2008 and the additional ones established by SAs which are "competent pursuant to Articles 55 or 56" under the consistency mechanism (in this regard both letters a) and b) of Article 43.1. and Article 43.3. refer expressly to Articles 55 or 56 GDPR). This mechanism, according to Articles 63 and 64.1.c) aims at ensuring the consistent application of the GDPR throughout the EU (see recital 135), i.e. that the accreditation requirements are in line with the GDPR, and does not entail any 'uniformity' or 'identity' of accreditation requirements for CBs which may differ among MS. Moreover, according to Art. 55.1 GDPR each SA is responsible for the fulfilment of the tasks and the exercise of the powers in its territory and, according to Art. 57.1.p) and q) GDPR, every SA in its territory is committed the task of establishing the requirements for accreditation of CBs (and eventually conducting accreditation of CBs pursuant to Article 43.1.a) GDPR and revoking it, according to Article 43.7 GDPR, along or not with the NAB).

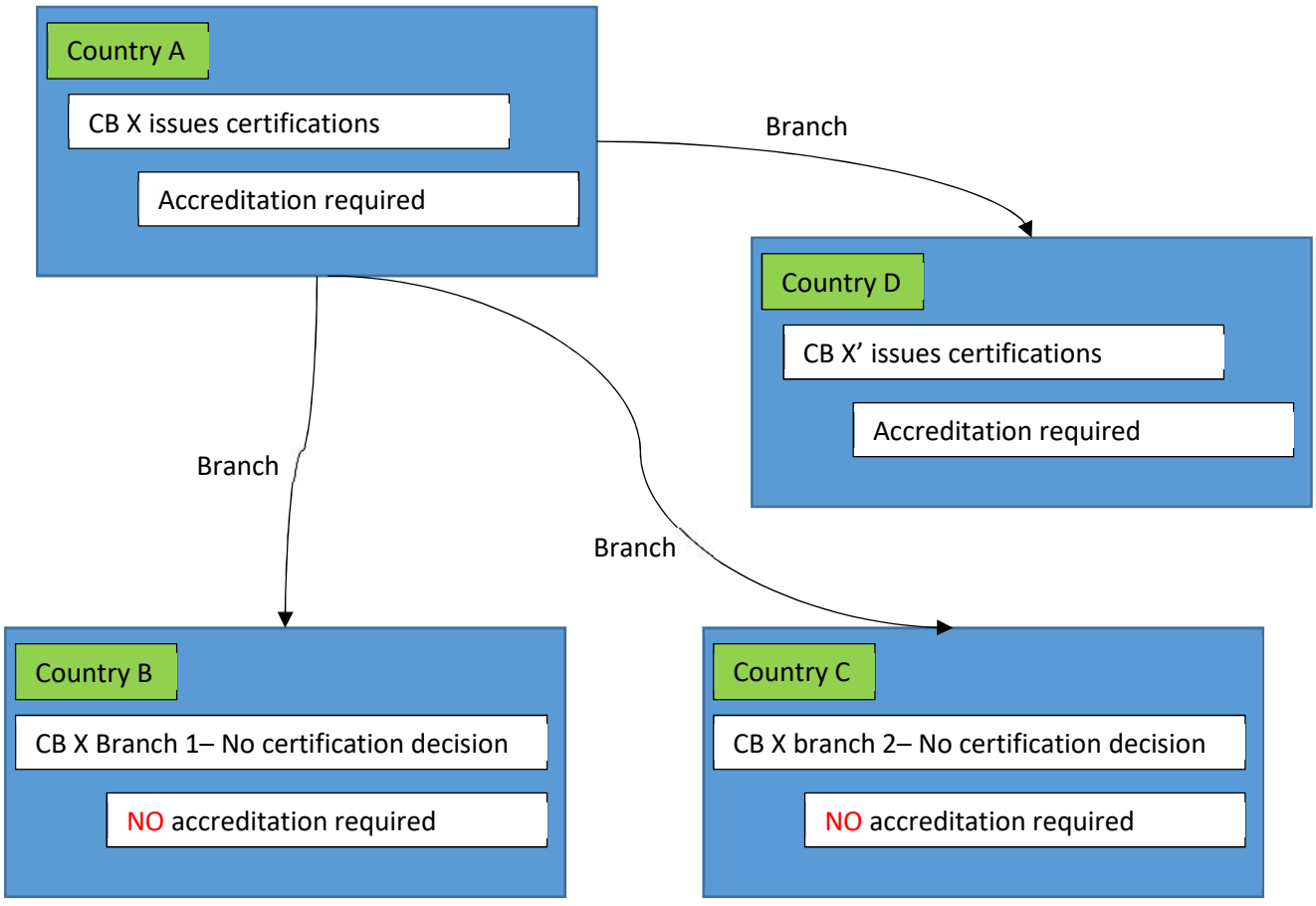
[16] As the accreditation requirements are consistent over the different countries, the risk of forum shopping for a certification body to be accredited is very low.

68. What would be the consequences if country B or country C do not adopt the certification criteria and the CB certifies an applicant in country B or C?

69. Nothing forbids the CB to certify an applicant in country B or C, however the SAs from country B or C would not recognize the certification criteria and therefore the certification would be useless.

10.2 Scenario 2: A certification body may have entities / branches in several member states of the EU.

70. Accreditation is required for the entities that are responsible for issuing the certification and managing the certification activities of its branches. If the branches are only doing support function (example: collect information, make on-site visits,…) and they do not perform certifications autonomously, they don't need an accreditation and cannot award certifications. However, they have to be taken into account in the accreditation phase of the 'main' entity to which they are attached.



10.3 Scenario 3: "Data controllers" may not be the same legal entity as the corporate entities of the organisation. "DataCompany Country A" may be the data controller for personal data processed by "DataCompany (sales) Country B".

71. Certificates can only be granted to controller and processor. In this scenario, if DataCompany Country A is the controller, it will have to request a certification. The certificate shall be delivered to the company that has control over the measures put in place to be compliant with the criteria.

72. If DataCompany (sales) Country B is qualified as a processor and the certification schemes is also adapted to and targeting the processor, DataCompany (sales) Country B could also apply for certification in their capacity as processor. Both controllers and processors may apply for certifications. Therefore, if there are certification schemes targeted both "for controllers" or "for processor" then "DataCompany Country A" can be certified for the former and "DataCompany (sales) Country B" for the latter.

10.4 Scenario 4: How to handle certification in a joint controllership scenario?

73. In the context of certification, the responsibilities in a joint controllership should be clarified in the joint controllership arrangement. The EDPB has adopted guidelines about how to setup such an arrangement: "Guidelines 07/2020 on the concepts of controller and processor in the GDPR.

Contractual agreement with the certification body:

74. The contractual agreement between a certification body and an applicant has to deal with responsibilities of each party regarding the activities to be certified.

75. To ensure clear transparency, a certificate in a joint controllership situation should mention the name all concerned joint controllers.

76. It is important that the complete scope of relevant processing (falling into the certification scope) has to be part of the ToE considerations and determination. Defining in the ToE partial processing that just belongs to one controller from the joint controllership may not be compatible with the certification mechanism.

Communication with the competent supervisory authority:

77. The EDPB guidelines 07/2020 on the concept of controller and processor in the GDPR mention that the "Joint controllers should organize in the arrangement the way they will communicate with the competent supervisory data protection authorities". Therefore, the arrangement should include a section that deals with the communication with the competent SA regarding certification in the joint controllership relation.

11 RELATION BETWEEN SA & NABS

78. CBs may apply for accreditation in relation to a specific certification scheme. The assessment of certification schemes is therefore closely linked with the accreditation of CBs which will may fall under the duty of the SA, the duty of the NAB or a combination of the SA / NAB, depending on the national legal framework. In this regard, it is important to regulate the cooperation between SAs and NABs with agreements that clearly identify the responsibilities of each party. From a SA point of view, it should be ensured that the agreement involves personnel with knowledge of certification mechanisms. From an NAB point of view, it should be ensured that the agreement involves personnel with knowledge of data protection compliance. In any case this assessment should take into account:

    - The scope and objectives of the certification schemes
    - The certification mechanisms and if applicable any combined ISO standard
    - The data protection compliance requirements