Comments by Cesare Gallotti about "Guidance on certification criteria assessment (Addendum to Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation)" (available on https://edpb.europa.eu/our-work-tools/documents/public-consultations/2021/guidance-certification-criteria-assessment_en).

Terminology ("Certification criteria" and others)

"Certification criteria" is a general term used in GDPR, but it is not defined.

It is important to define it because certification criteria include:

- product requirements (as required in ISO/IEC 17065, 3.8);
- audit procedures (including, for example, how to determine the ToE, check lists, methods of evaluation such as on-site inspections and code review, certification documentation, documentation of results);
- certification body procedures (EDPB Guidelines 1/2018 uses the term "certification procedures"), e.g. completing the certification agreement, paying fees, providing information about changes to the certified product, providing access to certified products for surveillance activities; they also include how to manage internal reviews and evaluations, and how to manage certificates (certification decision, directory, termination, reduction, suspension or withdrawal, competence of auditors, procedures for monitoring of adherence, reviewing, handling complaints, and withdrawal; language of the reports; "Procedures for the issuance and periodic review of certifications" as described in paragraph 61 of EDPB Guidelines 1/2018).

"Certification criteria", "certification mechanisms", "certification scheme" are used as interchangeable. The document should clearly state if they are the same or explain their relationships (and reviewed in order to ensure consistency).

In ISO/IEC 17065, the term "certification scheme" is used, in EDPB Guidelines 1/2018 the term "certification mechanism" is used (and "certification criteria" is a term used for "product requirements"). So we should provide a definition and relationships between the terms for giving clarity (and the terms should be uniformly used; in the current text the term "scheme criteria" is wrongly used instead of "certification criteria").

In all the document we should review the text because sometimes the term "certification criteria" is used for product requirements or for certification body procedures, without any consinstency.

Relationship with ISO/IEC 17067

The document should recall require the elements in paragraph 6.5.1 of ISO/IEC 17067. This will help the understanding of the document.

Those elements should be split between:

- product requirements (for the ToE);
- certification procedures (for the CB).

Scheme owners and certification criteria

We should say that scheme owners can adopt some criteria already written and published by other entities, e.g. standardization bodies.

This is also in EDPB Guidelines 1/2018 ("develop its own or adopt certification criteria").

So the text should be rewritten when some requirements for the scheme owners are in fact requirements for the certification criteria.

Scheme owner

We should have the opportunity to have accreditation bodies as scheme owners.

Should and shall

All the document does not use the "shall".

Therefore, also similar terms (e.g. "is to be", as in "Understanding how the ToE is to be selected and defined") should be avoided.

Levels of implementation and criteria levels (para 31)

In paragraph 31, the second list item says that "an evaluator can assess the processing objectively and to defined levels of implementation".

It is better to avoid to use the term "level" because there are assessments procedures and certification schemes that have levels of implementation (e.g. Common criteria or ISO/IEC 15408 have 7 assurance levels). In this case, it may be good to use "an evaluator can assess the processing objectively and the implementation of criteria".

Also "criteria levels" should be avoided.

Criteria and shall (para 37)

In 37.

The following example of criterion is not correct because the "shall" should be used: "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]".

It should be rewritten as follows: "when developing software, test data sets SHALL be composed of anonymized data or dummy data. Anonymization SHALL requires [conditions to be met]. Only if [conditions to be met] pseudonymized data SHALL allowed to be used. Pseudonymization SHALL require [conditions to be met]. If pseudonymization is to be used, [conditions to be met]".

Unclear items (para 38)

The following items in paragraph 38 are too vague:

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 nonconformity 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.*

I cannot propose an alternative because the requirements are too vague and I cannot understand what they mean.

Role of the auditor (para 38)

In paragraph 38, item 5 requires to the the auditor to describe the improvement actions, but an auditor cannot write improvement actions.

First example in paragraph 40

The first examples in paragraph 40 is unclear and too specific for a pseudonimization process:

1- it assumes that pseudonimization works only with encryption or hashing, but this is not true; also salting and splitting techniques can be used;
2- the required details are from a specific technology, so the scheme will only be applicable to one technology, but there are several good encryption and hashing algorithms, so a technical criterion should not require only one;
3- this is incompatible with requirement 57 of the EDPB Guidelines 1/2018 (*the scope of certification and criteria should not be so narrow as to exclude IT applications designed differently*).

Footnote 8 (para 44)

Note 8 says that "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)".

It is unclear what it means. And few things should be reviewed:

- PDCA is not "of ISO";
- the term "rules" is used, but without any context, so we don't understand what they are;
- the next sentence (about the "only one output") is not linked with the previous one.

Paragraph 47 unclear

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.

In the first sentence, we have an "as well as" when talking about certification and check list, but then it sais that "this means they are different". This is unclear.

Also, be aware that check lists are one method for verifications (and the verification is only one step of the certification).

Paragraph 52 unclear

This sentence is unclear:

“*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*”.