Guida - Addendum

(Allegato alle linee guida 1/2018 sulla certificazione e sull'identificazione dei criteri di certificazione in conformità agli articoli 42 e 43 del regolamento)

Valutazione dei criteri di certificazione

The Association Osservatorio679

Adottato il 06 aprile 2021

PARAGRAPH		NOTE
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.	The concept as expressed opens up potential subjectivity of evaluation that, because there is no balancing mechanism, could lead to differences in approval between SAs.
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;	The term "broad range" is not appropriate because it could result in discrimination among treatments. A general scheme in truth where all treatments are covered
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);	It's a poor example that tends to be misleading....
6	“Certification guidance” – assistance for auditors or implementers related to how criteria could be met under differing circumstances, scale or context.	The meaning of "guidance" for the use of the scheme is not clear. The auditor should identify the competences of the personnel involved in the certification process according to §6.1.2 of ISO 17065. In particular §6.1.2.1 a) and b) should be followed
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.	Leveling down to specific sector "commonly found risks" could divert criteria from main certification scope and objectives as set out in 5.1 Evaluating the Scope of a Certification Scheme - paragraph no.20 Besides, according to Section 6, paragraph no.31, "certification criteria need to be framed in such a way that the criteria are applicable to diverse contexts (sectorial context, technological context), including their scalability to meet the requirements of SMEs " GDPR Article 42 p.1 and p. 5 stress the importance to provide certification

	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.	mechanisms at EU level to comply with GDPR provisions; taking specifically onboard national regulations could lead to multiple and complicated groups of criteria, while adaptive criteria could just refer to national obligations and achieve needed flexibility to provide uniformity in EU member states, important to avoid patchy application The Audit will obviously have to be set up according to international standard rules and the GDPR must follow the readjusted ISO 19011. In particular, § 5.3 already indicates how audit-related risks are to be assessed and determined. Such an indication could be misleading and unclear as it happens regardless. It is the standard for conducting the audit that indicates this, not the scheme that must be structured in this way in the criteria.
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 Adopted - version for public consultation 6 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.	It is against the rules of product service certification and therefore contrary to the recital 100
50	The methodology proposed to demonstrate the compliance to the criteria in the context of national	Addressing a transparent and repeatable methodology to demonstrate compliance to criteria (which should be

	regulation shall be transparent and repeatable. For general certification schemes, elaborating specific criteria based on applicable national regulations might be highly complex9.	framed in a clear and consistent way, allowing flexible approach and repeatability and full GDPR compatibility) means to maintain a pretty high level of standardisation which cannot be found in the particular and not homogeneous context of national regulation, both for general or specific certification schemes. Paragraph no. 51 refers to possible means for scheme owners which are not applicable in practice or could lead to excessively long times for preparing the schemes, which are, on the other hand, urgent
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.	In relation to the purpose of certification, the criteria may, in the European Seal, differ in relation to different member states and different specific legislations: the point is conflicting not only on what is certification, but also in why a Regulation and not a Directive has been adopted. Finally, there is confusion between hard law and soft law.

Best regards,

The Association OSSERVATORIO679

Riccardo Giannetti
Cinzia Maria Gagliardi
Mazzoni fausto
Oliva Alessandro
Popoli Annarita
Posti Stefano
Martello Andrea