# EDPB Certification Guidelines

**Public Consultation: Comments submitted by SCOPE Europe bvba/sprl**

Published and Submitted: **10. July 2018**

## 1 About SCOPE Europe sprl

SCOPE Europe is a subsidiary of Selbstregulierung Informationswirtschaft e.V. (SRIW e.V.). SRIW e.V. is a Monitoring Body for Data Protection Code of Conducts in Germany since 2011. As the European General Data Protection Regulation shifts national approaches to a european framework, SCOPE Europe is intended to continue and compelement the portfolio of SRIW in Europe.

SCOPE Europe therefore has deep knowledge and experience in levelling industry and data subject needs and interests to credible and pragmatic but also rigoros provisions and controls. SCOPE Europe gained experience throughout multiple initiatives, discussions with different stakeholders of different kinds (e.g. consumer and data subject' interest groups, industry members, data protection authorities, legislators as well as legal experts of literature and practice). Based on this experience the following comments are made.

# Table of Contents

1 About SCOPE Europe sprl ..... 1

2 Preliminary Note ..... 3

3 Summary ..... 3

4 General Remarks ..... 3

5 Specific Remarks ..... 4

5.1 1.1 Scope of the Guidelines ..... 4

5.2 1.3.1. / 1.3.2 Interpretation of “certification” ..... 4

5.3 1.3.2 Certification mechanisms, seals and marks ..... 5

5.4 2.1 Supervisory Authority as certification body ..... 6

5.5 2.2 Supervisory Authority’s further tasks regarding certification ..... 6

5.6 3. The role of a certification body ..... 7

5.7 Specific Guidance for accreditation and assessment procedures ..... 8

5.8 4. The Approval of certification criteria ..... 8

5.9 4.3 The European Data Protection Scheme ..... 8

5.10 5. The development of certification criteria ..... 9

5.11 5.1. What can be certified under the GDPR? ..... 9

5.12 5.2 Determining the object of certification ..... 10

5.13 5.3. Evaluation methods and methodology of assessment ..... 10

5.14 5.4 Documentation of assessment ..... 10

5.15 5.5 Documents of results ..... 11

5.16 6 Guidance for defining certification criteria ..... 12

5.17 6.1 Existing standards ..... 13

5.18 6.2 Defining criteria ..... 13

## 2 Preliminary Note

On 30 May 2018, the European Data Protection Board (**EDPB**) published a public consultation on the *Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation 2016/679* (**Guidelines**).

As the EBPD invites all interested stakeholders to share their views and concerns, SCOPE Europe sprl decided to submit comments on the Guidelines as outlined on the website of the EDPB[1].

## 3 Summary

In general, the outlined concepts and aspects of the Guidelines and the covered sections are welcomed and highly appreciated. The purpose and scope are articulated clearly, also the given guidance can foster the implementation of Art. 42/43 in the market. Regarding the outlined aspects, this document highlights the importance of comparability and exclusivity of Certifications, as recommendations for clearer guidance on both concepts are given below. In addition, a clearer distinction between Certifications and Codes of Conduct pursuant to Art. 40/41 GDPR, for instance by preventing any confusing language or legal terms, within the Guidelines is recommended.

**Appreciated concepts** mentioned in the Guidance are

1. interoperability of existing and upcoming standards and certification schemes
2. transparency and hence comparability between certificates
3. consistency of guidance when approving or defining certification criteria

**Recommendations** are

1. preventing confusions between Certifications and Codes of Conduct
2. further precision and guidance to safeguard comparability, transparency and finally credibility of Certifications
3. creating awareness and certainty among market players regarding certification seals or marks

## 4 General Remarks

The Guidelines are highly appreciated. The Guidelines elaborate purpose and necessity within themselves, as they intent to *"help Member States, supervisory authorities and national accreditation*

[1] European Data Protection Board, accessed on July 3, 2018: https://edpb.europa.eu/our-work-tools/public-consultations-art-704_en

*bodies establish a more consistent, harmonised approach for the implementation of certification mechanisms in accordance with the GDPR.“* This is also very much welcomed as the general scope and extent of GDPR create a degree of uncertainty in the market. Therefore, additional guidance as given within the Guidelines is both helpful and relevant.

Certification, as well as other mechanisms like Codes of Conduct will only take effect if and so far these mechanisms are both transparent and reliable. The Guidelines perfectly point out the necessity and main aspects of transparency:

> *Since certification does not prove compliance in and of itself but rather forms an element that can be used to demonstrate compliance, it should be produced in a transparent manner. Demonstration of compliance requires supporting documentation, specifically written reports which not only repeat but describe how the criteria are met and 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. (1.2 of the Guidelines)*

# 5 Specific Remarks

In addition to the General Remarks, please find following some more specific comments:

## 5.1 1.1 Scope of the Guidelines

> *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). (1.1 of the Guidelines)*

Additional guidance on third country transfers would be much appreciated and helpful, also taking into consideration the specific distinctions for appropriate safeguards (e.g. Codes of Conduct vs. Certification vs. Binding Corporate Rules vs. Standard Data Protection Clauses).

## 5.2 1.3.1. / 1.3.2 Interpretation of “certification”

> *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”. (1.3.1 of the Guidelines)*

> *A certificate is a statement of conformity. 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 documents such as regulations, standards or technical specifications. (1.3.2 of the Guidelines)*

It is of high importance to prevent any confusion in the market. Therefore, GDPR should not interpret and use international standard terminology differently. At the same time, it is of utmost importance to prevent GDPR Certifications from losing their benefits for those trusting in them. Hence, Certifications must ensure that

1. principally identical findings result in principally identical attestations,

2. market is not flooded by too many Certifications with mainly identical scopes.

Additionally, Guidelines for Certification as well as for Codes of Conduct should not confuse the market. Guidance should not unnecessarily equate both mechanisms, as this will finally erode the one or the other.

## 5.3 1.3.2 Certification mechanisms, seals and marks

> *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 documents such as regulations, standards or technical specifications. These requirements in the context of certification under the GDPR are set out in the additional requirements that supplement the rules for accreditation of certification bodies in EN-ISO/IEC 17065/2012 and the certification criteria approved by the competent supervisory authority or the Board. 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 (1.3.2 of the Guidelines).*

In general, Certifications are relevant for the market if

1. the certification criteria create a certain level of exclusivity, meaning that the requirements of the seal or mark guarantee a high-quality assessment of the subject matter,
2. all stakeholders are aware of the content and structure of the seal or mark, meaning the precise assessment conditions are communicated publicly and transparent to the market.

## 5.4 2.1 Supervisory Authority as certification body

> *[...] 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))[...]*
>
> *[...] 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).*

This paragraph uses language that is principally linked to Codes of Conduct pursuant to Art. 41 GDPR, e.g. the terminology "monitoring". In order to prevent uncertainties and confusion between Codes of Conduct and Certification, the language that is linked to Codes of Conduct should never be used in the context of Certification and vice versa. Instead of "monitoring" the Guidelines should use "periodic review" as pursuant to Article 43 GDPR (as quoted in the sentence above). The distinction between Art. 40/41 GDPR and 42/43 GDPR is mandatory, notably because Codes of Conduct are based on plausibility supplementing by a constant monitoring, while Certificates shall include a final assessment of all criteria at a certain, distinct time.

## 5.5 2.2 Supervisory Authority's further tasks regarding certification

> *[...] 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.*

First, comparability of Certifications should be an overall priority. The purpose of Certification under GDPR can only be achieved meaningfully if a certification scheme is as clear and reproducible as possible; i.e. the outcome of the certification process must be the same, regardless of the certifier or auditor.

Therefore, it is highly appreciated that the Guidelines already address specific procedures to keep Certification comparable, transparent and reliable.

Second, certification schemes should re-use existing schemes and common standards as far as possible. Where current certification schemes are covering relevant aspects, compliance should be possible to prove according to respective implemented measures that are considered compliant with international common standards. Where existing schemes are lacking relevant aspects under GDPR, specific GDPR schemes should focus on developing and evolving assessments covering those gaps. GDPR Certification additionally should focus on the effectiveness of implemented measures. Certifications simply covering the theoretical existence of privacy-related measures but without any assessment, whether those have the intended effect, seem to be without benefit for those trusting into certificates.

## 5.6 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 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).*

This paragraph uses language that is principally linked to Codes of Conduct pursuant to Art. 41 GDPR, e.g. the terminology "monitoring". In order to prevent uncertainties and confusion between Codes of Conduct and Certification, the language that is linked to Codes of Conduct should never be used in the context of Certification and vice versa. Instead of "monitoring" the Guidelines should use "periodic review" as pursuant to Article 43 GDPR. The distinction between Art. 40/41 GDPR and 42/43 GDPR is mandatory, notably because Codes of Conduct are based on plausibility supplementing by a constant monitoring, while certificates shall include a final assessment of all criteria at a certain, distinct time.

## 5.7 Specific Guidance for accreditation and assessment procedures

> *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. (3. of the Guidance)*

To prevent confusion between Codes of Conduct and Certifications and to keep Certifications comparable, transparent and finally reliable, detailed guidance for specific assessments is helpful. The market considers Certifications to be full coverage assessments. Certificates principally confirm processes and hard facts, solely verifying if a process exists and that related actions probably occur. It principally does not - and to a certain extent cannot - verify if the process is or will actually be started or if it will be complied with. Both are examples potentially covered by Codes of Conduct. In comparison to Certifications, Codes of Conduct can confirm that a certain process takes place if conditions agreed-on are established.

However, guidance should safeguard that every Certification is complemented by an audit procedure that – to the extent possible – verifies the effectiveness of the implemented measures and procedures.

## 5.8 4. The Approval of certification criteria

> *[...] to contribute to the consistent application of the GDPR.*

As highlighted already, consistency is key. Certification criteria should only be approved if the requirements and procedures are as precise as possible to safeguard consistent, transparent, comparable and by this reliable assessments and Certifications.

## 5.9 4.3 The European Data Protection Scheme

> *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.*

Avoiding fragmentation, especially given existing certification schemes, is welcomed. This should be pursued in the overall approach of the EPDB on Art. 42/43 GDPR.

## 5.10 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.*

It is crucial that there is no confusion between Certificates and Codes of Conduct. Both should be strictly separated because of their different characters. This difference should be marked, inter alia through language.

Certificates principally confirm processes and hard facts, solely verifying if a process exists and that related actions probably occur. It principally does not and to a certain extent cannot verify if the process is or will actually be started or if it will be complied with. However, guidance should safeguard that every Certification is complemented by an audit procedure that as much as possible verifies the effectiveness of the implemented measures and procedures.

Whether processes are implemented into daily business and complied with over time may also be assessed by Codes of Conduct. In comparison to Certifications, Codes of Conduct e.g. can confirm that a certain process takes place if conditions agreed-on are established.

## 5.11 5.1. What can be certified under the GDPR?

> *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.*

To raise awareness within the target group of Certifications (i.e. both providers and customers) regarding the difference between Certifications and Codes of Conduct it is recommended to clearly distinguish between the requirements of Certifications and Codes of Conducts and their intended use cases.

Unfortunately, there is already confusion within the market regarding the accreditation and conformity against ISO 17065. This adherence is required for certification bodies, but explicitly not for monitoring

bodies of Codes of Conduct. This distinction within the legal framework should be elaborated within the guidance. The requirement of ISO-conformity of certifications bodies should be linked with specific requirement of Certification.

## 5.12 5.2 Determining the object of certification

> *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.*

It is highly appreciated to make a clear description of included processing operations. Transparently communicating these operations helps generally to easily compare existing certificates. Such a transparent and publicly available documentation will also prevent misuse of Certifications as it happens – to some extent – today. Services that are only partially certified should not be able to create the wrongful impression that these services are fully certified by simply attaching a certification mark or seal to the service.

Scopes which are not part of Certifications could be covered by other alternatives such as Codes of Conduct.

## 5.13 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.*

Again, it is to highlight that comparability is guaranteed. This should be reflected in all methods and mechanisms for evaluation.

## 5.14 5.4 Documentation of assessment

> *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.*

It is highly appreciated that documentation shall provide transparency. It is important, as stated in the Guidelines, that the publicly available evaluation allows comparison of the individual certificates. This perfectly highlights the unequivocally necessary comparability.

Additionally, guidance should clarify that certifiers and auditors must not prevent their findings and reports to be published or communicated to interested parties; e.g. under copyright law. Today, the latter sometimes prevents certified entities to transparently communicate their compliance to interested parties as they are only allowed to share the certification mark or seal but not any documented findings and reports.

> *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.*

The given guidance is fully supported. Procedures to review Certifications must ensure they are both comparable and transparent in documentation. This is a predominant requirement to level and verify quality of Certifications.

## 5.15 5.5 Documents of results

> *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 [...]*

Again, the mentioned points within the Guidelines should be supplemented with the point of comparability of certificates. Especially for Data Subjects it is important to easily figure out which certificates

are relevant for them. Hence, it is mandatory that Data Subject can recognize different certificates and be certain about the respective scope by means of comparable certification mechanisms and transparent procedures.

## 5.16 6 Guidance for defining certification criteria

> *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.*

Those cited points are highly appreciated findings within the Guidelines. Additionally, interoperability with Codes of Conduct should be reflected as Certifications and Codes of Conduct are both accepted and equal mechanisms under GDPR to demonstrate compliance. The requirement of the flexibility and scalability to different types and sizes of organisations is appreciated. Codes of Conduct and Certifications may also complement each other, as mentioned throughout this consultation repeatedly, the alignment would address both: recognition in the market and applicability to SMEs.

> *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.*

Considering the differences between sizes of companies is appreciated. Especially on those different levels, a transparent and comparable certification mechanism is important to foster trust, compliance and keep certificates competitive in the sense of credibly increasing the data protection level.

## 5.17 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.*

It is highly appreciated to refer to existing standards that can help meeting obligations under GDPR and define the requirement of keeping those standards interoperable. It is recommended to additionally and explicitly refer to Codes of Conduct. Under GDPR, Codes of Conduct are recognized as an equal instrument to demonstrate adherence to obligations under GDPR. To prevent this legally strengthened tool, i.e. Codes of Conduct, from being supressed by Certifications, EDPB should prevent statements that reinforce restraints that have been passed throughout the legislative process. Again, such a clarification could communicate the difference of Certificates and Codes of Conduct.

## 5.18 6.2 Defining criteria

> *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.*

Application to different scenarios requires a structure of procedures of Certifications which allow to compare the procedures of certificates in certain details. A missing comparability would give rise to a significant risk of a lack of clarity and would not be helpful neither for those being certified nor for data subjects.