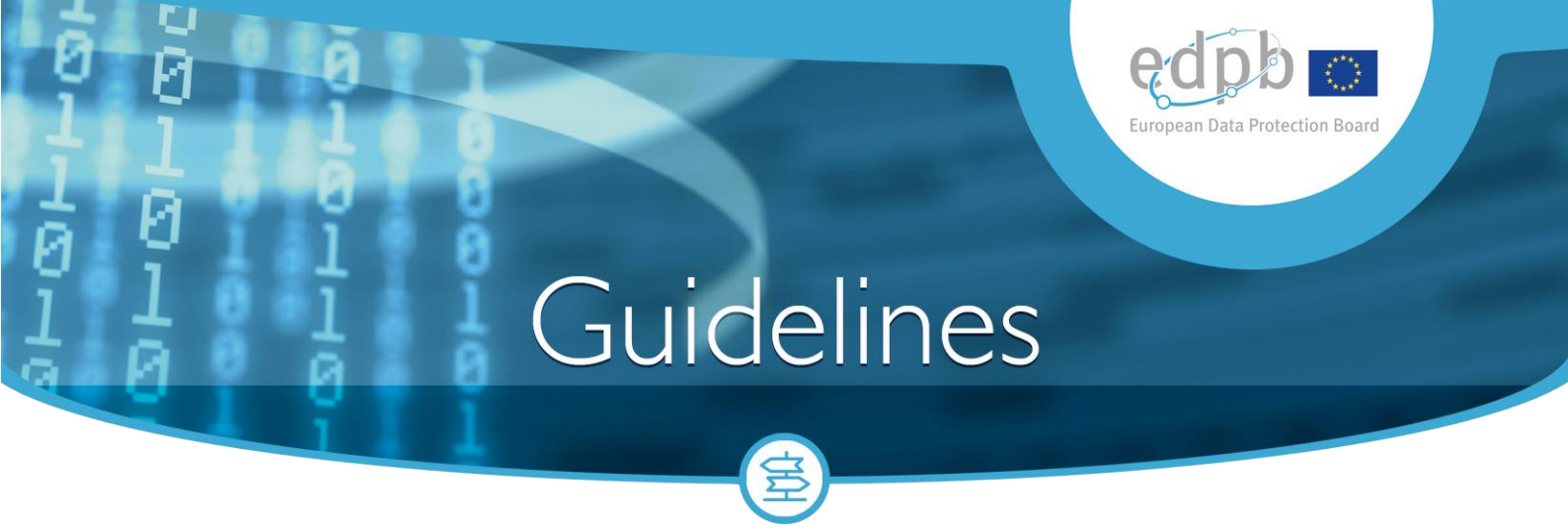

Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation (2016/679)

Adopted on 4 December 2018

Contents

The European Data Protection Board

Having regard to Article 70 (1)(e) of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC,

HAS ADOPTED THE FOLLOWING GUIDELINES

1 INTRODUCTION

The General Data Protection Regulation (Regulation (EU) 2016/679) ('the GDPR'), which comes into effect on 25 May 2018, provides a modernised, accountability and fundamental rights based compliance framework for data protection in Europe. A range of measures to facilitate compliance with the provisions of the GDPR are central to this new framework. These include mandatory requirements in specific circumstances (including the appointment of Data Protection Officers and carrying out data protection impact assessments) and voluntary measures such as codes of conduct and certification mechanisms.

As part of establishing certification mechanisms and data protection seals and marks, Article 43(1) of the GDPR requires Member States ensure that certification bodies issuing certification under Article 42(1) are accredited by either or both, the competent supervisory authority or the national accreditation body. If accreditation is carried out by the national accreditation body in accordance with ISO/IEC 17065/2012, the additional requirements established by the competent supervisory authority must also be applied.

Meaningful certification mechanisms can enhance compliance with the GDPR and transparency for data subjects and in business to business (B2B) relations, for example between controllers and processors. Data controllers and processors will benefit from an independent third-party attestation for the purpose of demonstrating compliance of their processing operations.[1]

In this context, the European Data Protection Board (EDPB)recognizes that it is necessary to provide guidelines in relation to accreditation. The particular value and purpose of accreditation lies in the fact that it provides an authorative statement of the competence of certification bodies that allows the generation of trust in the certification mechanism.

The aim of the guidelines is to provide guidance on how to interpret and implement the provisions of Article 43 of the GDPR. In particular, they aim to help Member States, supervisory authorities and national accreditation bodies establish a consistent, harmonised baseline for the accreditation of certification bodies that issue certification in accordance with the GDPR.

[1] Recital 100 of the GDPR states that the establishment of certification mechanisms can enhance transparency and compliance with the Regulation and allow data subjects to assess the level of data protection of relevant products and services.

2 SCOPE OF THE GUIDELINES

These guidelines:

- set out the purpose of accreditation in the context of the GDPR;
- explain the routes that are available to accredit certification bodies in accordance with Article 43(1), and identify key issues to consider;
- provide a framework for establishing additional accreditation requirements when the accreditation is handled by the national accreditation body; and
- provide a framework for establishing accreditation requirements, when the accreditation is handled by the supervisory authority.

The guidelines do not constitute a procedural manual for the accreditation of certification bodies in accordance with the GDPR. They do not develop a new technical standard for the accreditation of certification bodies for the purposes of the GDPR.

The guidelines are addressed to:

- Member States, who must ensure that certification bodies are accredited by the supervisory authority and/or the national accreditation body;
- national accreditation bodies that conduct the accreditation of certification bodies under Article 43(1)(b);
- the competent supervisory authority specifying 'additional requirements' to those in ISO/IEC 17065/2012[2] when the accreditation is carried out by the national accreditation body under Article 43(1)(b);
- the EDPB when issuing an opinion on and approving competent supervisory authority accreditation requirements pursuant to Articles 43(3), 70(1)(p) and 64(1)(c);
- the competent supervisory authority specifying the accreditation requirements when accreditation is carried out by the supervisory authority under Article 43(1)(a);
- other stakeholders such as prospective certification bodies or certification scheme owners providing for certification criteria and procedures[3].

Definitions

The following definitions seek to promote a common understanding of the basic elements of the accreditation process. They should be considered as points of reference and they do not raise any claim to be unassailable. These definitions are based on existing regulatory frameworks and standards, especially on the relevant provisions of GDPR and ISO/IEC 17065/2012.

[2] International Organization for Standardization: Conformity assessment -- Requirements for bodies certifying products, processes and services.

[3] Scheme owner is an identifiable organisation which has set up certification criteria and the requirements against which conformity is to be assessed. The accreditation is of the organisation that carries out assessments (Article 43.4) against the certification scheme requirements and issues the certificates (i.e. the certification body, also known as conformity assessment body). The organisation carrying out the assessments could be the same organisation that has developed and owns the scheme, but there could be arrangements where one organisation owns the scheme, and another (or more than one other) performs the assessments.

For the purposes of these guidelines the following definitions shall apply:

'*accreditation*' of certification bodies see section 3 on interpretation of accreditation for the purposes of Article 43 of the GDPR;

'*additional requirements*' means the requirements established by the supervisory authority which is competent and against which an accreditation is performed[4];

'*certification*' shall mean the assessment and impartial, third party attestation[5] that the fulfilment of certification criteria has been demonstrated;

'*certification body*' shall mean a third –party conformity assessment[6] body[7] operating a certification mechanisms[8];

'*certification scheme*' shall mean a certification system related to specified products, processes and services to which the same specified requirements, specific rules and procedures apply;[9]

'criteria' or certification criteria shall mean the criteria against which a certification (conformity assessment)is performed;[10]

'national accreditation body' shall mean the sole body in a Member State named in accordance with Regulation (EC) No 765/2008 of the European Parliament and the Council that performs accreditation with authority derived from the State[11].

3 INTERPRETATION OF 'ACCREDITATION' FOR THE PURPOSES OF ARTICLE 43 OF THE GDPR

The GDPR does not define 'accreditation'. Article 2 (10) of Regulation (EC) No 765/2008, which lays down general requirements for accreditations, defines accreditation as

"an attestation by a national accreditation body that a conformity assessment body meets the requirements set by harmonised standards and, where applicable, any additional requirements including those set out in relevant sectoral schemes, to carry out a specific conformity assessment activity "

Pursuant to ISO/IEC 17011

[4] Article 43(1), (3) and (6).
[5] Note that according to ISO 17000, third-party attestation (certification) is "applicable to all objects of conformity assessment" (5.5) "except for conformity assessment bodies themselves, to which accreditation is applicable" (5.6).
[6] Third-party conformity assessment activity is performed by an organisation that is independent of the person or organization that provides the object, and of user interests in that object, cf. ISO 17000, 2.4.
[7] See ISO 17000, 2.5: "body that performs conformity assessment services"; ISO 17011: "body that performs conformity assessement services and that can be the object of accreditation"; ISO 17065, 3.12.
[8] Article 42.1, 42.5 GDPR.
[9] See 3.9 in conjuction with Annex B of ISO 17065.

[10] See Article 42(5).
[11] See Article 2.11 765/2008/EC.

"accreditation refers to third-party attestation related to a conformity assessment body conveying formal demonstration of its competence to carry out specific conformity assessment tasks."

Article 43(1) provides:

"Without prejudice to the tasks and powers of the competent supervisory authority under Articles 57 and 58, certification bodies which have an appropriate level of expertise in relation to data protection shall, after informing the supervisory authority in order to allow it to exercise its powers pursuant to point (h) of Article 58(2) where necessary, issue and renew certification. Member States shall ensure that those certification bodies are accredited by one or both of the following:

(a) the supervisory authority which is competent pursuant to Article 55 or 56;
(b) the national accreditation body named in accordance with Regulation (EC) No 765/2008 of the European Parliament and of the Council in accordance with ISO/IEC 17065/2012 and with the additional requirements established by the supervisory authority which is competent pursuant to Article 55 or 56."

In respect of the GDPR, the accreditation requirements will be guided by:

- ISO/IEC 17065/2012 and the 'additional requirements' established by the supervisory authority which is competent in accordance with Article 43 (1)(b), when the accreditation is carried out by the national accreditation body and by the supervisory authority, when it carries out the accreditation itself.

In both cases the consolidated requirements must cover the requirements mentioned in Article 43(2).

The EDPB acknowledges that the purpose of accreditation is to provide an authoritative statement of the competence of a body to perform certification (conformity assessment activities)[12]. Accreditation in terms of the GDPR shall be understood to mean the following:

an attestation[13] by a national accreditation body and/or by a supervisory authority, that a certification body[14] is qualified to carry out certification pursuant to Article 42 and 43 GDPR, taking into account ISO/IEC 17065/2012 and the additional requirements established by the supervisory authority and or by the Board.

4 ACCREDITATION IN ACCORDANCE WITH ARTICLE 43(1) GDPR

Article 43(1) recognises that there are several options for the accreditation of certification bodies. The GDPR requires supervisory authorities and Members States to define the process for the accreditation of certification bodies. This section sets out the routes for accreditation provided in Article 43.

[12] Cf. Recital 15 765/2008/EC.
[13] Cf. Article 2.10 Regulation (EC) 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products.
[14] Cf. with the definition of the term "accreditation" pursuant to ISO 17011.

4.1 Role for Member States

Article 43(1) requires Member States *to ensure* that certification bodies are accredited, but allows each Member State to determine who should be responsible to conduct the assessment leading to accreditation. On the basis of Article 43(1), three options are available; accreditation is conducted:

(1) solely by the supervisory authority, on the basis of its own requirements;
(2) solely by the national accreditation body named in accordance with Regulation (EC) 765/2008 and on the basis of ISO/IEC 17065/2012 and with additional requirements established by the competent supervisory authority; or
(3) by both the supervisory authority and the national accreditation body (and in accordance with all requirements listed in 2 above).

It is for the individual Member State to decide whether the national accreditation body or the supervisory authority or both together will carry out these accreditation activities but in any case it should ensure that adequate resources are provided[15].

4.2 Interaction with Regulation (EC) 765/2008

The EDPB notes that Article 2(11) of Regulation (EC) No 765/2008 defines a national accreditation body as "the *sole* body in a Member State that performs accreditation with authority derived from the State".

Article 2(11) could be seen as inconsistent with Article 43(1) of the GDPR, which allows accreditation by a body other than the national accreditation body of the Member State. The EDPB considers that the intention of the EU legislation has been to derogate from the general principle that the accreditation be conducted exclusively by the national accreditation authority, by giving supervisory authorities the same power as regards the accreditation of certification bodies. Hence Article 43(1) is lex specialis vis-a-vis Article 2(11) of Regulation 765/2008.

4.3 The role of the national accreditation body

Article 43(1)(b) provides that the national accreditation body will accredit certification bodies in accordance with ISO/IEC 17065/2012 and the additional requirements established by the competent supervisory authority.

For clarity, the EDPB notes that the specific reference to 'to point (b) of paragraph 1 Article 43(3) implies that 'those requirements' points to the 'additional requirements' established by the competent supervisory authority under Article 43(1)(b) and the requirements set out in Article 43(2).

In the process of accreditation, the national accreditation bodies shall apply the additional requirements to be provided by the supervisory authorities.

A certification body with existing accreditation on the basis of ISO/IEC 17065/2012 for non-GDPR related certification schemes that wishes to extend the scope of its accreditation to cover certification issued in accordance with the GDPR will need to meet the additional requirements established by the supervisory authority if accreditation is handled by the national accreditation body. If accreditation for certification under the GDPR is only offered by the competent supervisory authority, a certification

[15] See Article 4(9) of Regulation (EC) 765/2008.

body applying for accreditation will have to meet the requirements set by the respective supervisory authority.

4.4 The role of the supervisory authority

The EDPB notes that Article 57(1)(q) provides that the supervisory authority *shall* conduct the accreditation of a certification body pursuant to Article 43 as a 'supervisory authority task' pursuant to Article 57 and Article 58(3)(e) provides that the supervisory authority has the authorisation and advisory power to accredit certification bodies pursuant to Article 43. The wording of Article 43(1) provides some flexibility and the supervisory authority's accreditation function should be read as a task only where appropriate. Member State law may be used to clarify this point. Yet, in the process of accreditation by a national accreditation body the certification body is required by Article 43(2)(a) to demonstrate their independence and expertise to the satisfaction of the competent supervisory authority in relation to the subject-matter of the certification mechanism it offers.[16]

If a Member State stipulates that the certification bodies are to be accredited by the supervisory authority, the supervisory authority should establish accreditation requirements including, but not limited to the requirements detailed in Article 43(2). In comparison to the obligations relating to the accreditation of certification bodies by national accreditation bodies, Article 43 provides less instruction about the requirements for accreditation when the supervisory authority conducts the accreditation itself. In the interests of contributing to a harmonised approach to accreditation, the accreditation criteria used by the supervisory authority should be guided by ISO/IEC 17065 and should be complemented by the additional requirements a supervisory authority establishes pursuant to Article 43(1)(b). The EDPB notes that Article 43(2)(a)-(e) reflect and specifiy requirements of ISO 17065. which will contribute to consistency.

If a Member State stipulates that the certification bodies are to be accredited by the national accreditation bodies, the supervisory authority should establish additional requirements complementing the existing accreditation conventions envisaged in Regulation (EC) 765/2008 (where Articles 3-14 relate to the organisation and operation of accreditation of conformity assessment bodies) and the technical rules that describe the methods and procedures of the certification bodies. In light of this, Regulation (EC) 765/2008 provides further guidance: Article 2(10) defines accreditation and refers to 'harmonized standards' and 'any additional requirements including those set out in relevant sectoral schemes'. It follows that the additional requirements established by the supervisory authority should include specific requirements and be focused on facilitating the assessment, amongst others, of the independence and level of data protection expertise of certification bodies, for example, their ability to evaluate and certify personal data processing operations by controllers and processors pursuant to Article 42.(1). This includes competence required for sectoral schemes, and with regard to the protection of fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.[17] The annex to these guidelines can help inform competent supervisory authorities when establishing the 'additional requirements' in accordance with Articles 43(1)(b) and 43(3).

[16] The additional requirements established by the supervisory authority pursuant to Article 43(1)(b) should specify requirements for independence and expertise. See also Annex 1 of the guidelines.
[17] Article 1(2) GDPR.

Article 43(6) provides that "[t]he requirements referred to in paragraph 3 of this Article and the certification criteria referred to in Article 42(5) shall be made public by the supervisory authority in an easily accessible form". Therefore, to ensure transparency, all criteria and requirements approved by a supervisory authority shall be published. In terms of quality and trust in the certification bodies, it would be desirable, if all the requirements for accreditation were readily available to the public.

4.5 Supervisory authority acting as certification body

Article 42(5) provides that a supervisory authority may issue certifications, but the GDPR does not require it to be accredited to meet the requirements under Regulation (EC) 765/2008. The EDPB notes that Article 43(1)(a) and specifically Article 58(2)(h), 3(a, e-f) empower supervisory authorities to perform both accreditation and certification, and at the same time provide advice, and, where applicable, withdraw certifications, or order certification bodies to not issue certifications.

There may be situations where the separation of accreditation and certification roles and duties is appropriate or required, for example, if a supervisory authority and other certification bodies co-exist in a Member State and both issue the same range of certifications. Supervisory authorities should therefore take sufficient organisational measures to separate the tasks under the GDPR to anchor and facilitate certification mechanisms while taking precautions to avoid conflicts of interest that may arise from these tasks. Additionally, Member States and supervisory authorities should keep in mind the harmonised European level when formulating national law and procedures relating to accreditation and certification in accordance with the GDPR.

4.6 Accreditation requirements

The annex to these guidelines provides guidance on how to identify additional accreditation requirements. It identifies the relevant provisions in the GDPR and suggests requirements that supervisory authorities and national accreditation bodies should consider to ensure compliance with the GDPR.

As established above, where certification bodies are accredited by the national accreditation body pursuant to regulation (EC) 765/2008, ISO/IEC 17065/2012 will be the relevant accreditation standard complemented by the additional requirements established by the supervisory authority. Article 43(2) reflects generic provisions of ISO/IEC 17065/2012 in the light of fundamental rights protection under the GDPR. The framework in the annex uses Article 43(2) and ISO/IEC 17065/2012 as a basis for the identification of requirements plus further criteria relating to the assessment of the data protection expertise of certification bodies and their ability to respect the rights and freedoms of natural persons with respect to the processing of personal data as enshrined in the GDPR. The EDPB notes that it is especially focused on ensuring that certification bodies have an appropriate level of data protection expertise in accordance with Article 43(1).

The additional accreditation requirements established by the supervisory authority will apply to all certification bodies requesting accreditation. The accreditation body will evaluate whether that certification body is competent to carry out the certification activity in line with the additional requirements and the subject-matter of certification. There shall be references specific sectors or areas of certification for which the certification body is accredited.

The EDPB also notes that the special expertise in the field of data protection is also required in addition to ISO/IEC 17065/2012 requirements, if other, external bodies, such as laboratories or auditors, perform parts or components of certification activities on behalf of an accredited certification body. In

these cases, accreditation of these external bodies under the GDPR itself is not possible. However, in order to ensure the suitability of these bodies for their activity on behalf of the accredited certification bodies, it is necessary for the accredited certification body to ensure that the data protection expertise required for the accredited body must also be in place and demonstrated with the external body with respect to the relevant activity performed.

The framework for identifying the additional accreditation requirements as presented in the annex to these guidelines does not constitute a procedural manual for the accreditation process performed by the national accreditation body or the supervisory authority. It provides guidance on structure and methodology and thus a toolbox to the supervisory authorities to identify the additional requirements for accreditation.

For the European Data Protection Board

The Chair

(Andrea Jelinek)