Requirements for Accreditation in Accordance with Art. 43(3) GDPR in Conjunction with DIN EN ISO/IEC 17065

Submitted by the German Data Protection Authorities (Länder and Bund)

Version 1.4 (08.10.2020)

Explanatory Notes and Draft

Explanatory Notes

General Notes

In the following, the requirements of DIN EN ISO/IEC 17065 based on Art. 43(3) GDPR in connection with Art. 57(1)(p) GDPR will be amended and specified by the German data protection supervisory authorities.[1]

The specific data protection requirements of Art. 42, 43 GDPR and the requirements of DIN EN ISO/IEC 17065 must be taken into account. Also "EDPB Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation (2016/679)" has been considered.

As an accreditation body, the DAkkS accredits the certification bodies together with the competent data protection supervisory authority. The competent data protection supervisory authority shall authorize the certification body to operate. This authorization is granted in an independent procedure on the basis of this joint accreditation.

The application for accreditation is submitted in writing to the DAkkS, which makes available an appropriate form. The DAkkS shall immediately inform the competent supervisory authority of the application and send the relevant documents.

The certification body certifies the products, processes and services of its clients insofar as these are processing operations according to the GDPR.

To prepare for accreditation, the certification body or the scheme owner must prepare a certification scheme and have it tested for suitability by the DAkkS in accordance with DIN EN ISO/IEC 17011:2017 (cf. DAkkS Rule 71 SD 0016). This certification scheme essentially contains the certification criteria for the implementation of the data protection legal requirements, which according to Art. 57 (1)(n) GDPR in conjunction with Art. 42(5) GDPR must either be approved by the competent data protection supervisory authority or (as a rule via the competent supervisory authority) transmitted to the European Data Protection Board for approval in accordance with Art. 63, 64(1)(c) GDPR.

If the criteria pursuant to Art. 57(1)(n) GDPR in conjunction with Art. 42(5) GDPR, are solely approved by the competent data protection supervisory authority, this authority shall forward the criteria to the European Data Protection Board in accordance with Art. 43(6.2) GDPR.

The certification schemes, including the approved criteria pursuant to Art. 42(5) GDPR, shall be published in the scheme database www.dakks.de.

[1] The requirements defined in EN ISO/IEC 17065, as well as the amendments to these requirements laid down by the data protection authorities in this document, shall be complied with by the certification body. The compliance has to be proved within the accreditation procedure.

With regard to the requirements for these criteria, reference is made to the document "Guidelines 1/2018 on certification and identifying certification criteria in accordance with Art. 42 and 43 of the Regulation 2016/679".

Specific Notes

The following document specifies the requirements of DIN EN ISO/IEC 17065 based on Art. 43(3) GDPR in connection with Art. 57(1)(p) GDPR by the German data protection supervisory authorities.

It references to the chapters 3 (terms and definitions), 4 (general requirements), 5 (structural requirements), 6 (Resource requirements), 7 (process requirements) and 8 (management system requirements) of the DIN EN ISO/IEC 17065.

The adapted chapters and passages are declared. Where necessary a substantiation is included.

General

Scopes of Accreditation (Scopes)

This document does not specify scopes for the accreditation of certification bodies. However, the certification bodies must define and precisely describe the scope of the certification program when submitting the application for program review. The certification program also specifies the required professional experience and expertise of the assessor for the specified areas of application.

Duration of Accreditation

Accreditation is limited to a maximum of five years pursuant to Art. 43(3) GDPR.

Specific references to DIN EN ISO/IEC 17065

I. Chapter 3: Definitions

3.4 Product, 3.5 Process and 3.6 Service (subject-matter of certification)

Permissible are certification schemes that consider processing operations, which are performed in products, processes and services or with the aid of (even several) products and services and that directly or indirectly confirm compliance with the provisions of the GDPR to the controller or processor.

The subject-matter of certification must meet the requirements of DIN EN ISO/IEC 17065. Thus management systems for the control of data processing are excluded as the subject of certification. Management systems are considered as part of a certification mechanism under the conditions set out in Chapter 7, note 7.4. The subject-matter of certification must also relate to data processing operations.

II. Chapter 4: General Requirements

Regarding 4.1 Legal and contractual matters

In addition to the legal responsibility of a certification body, accreditation shall ensure that a certification body is at all times able to demonstrate compliance with the terms of accreditation and its application of the GDPR to client organisations, client organisation's personal data and in respect of its own data controller obligations.

Regarding 4.1.2.2 Certification agreement

The minimum requirements for a certification agreement (contract between certification body and client) are to be amended by the following points:

1. The client's obligation to permanently fulfill the general certification requirements according to 4.1.2.2(a) must (equivalent to the regulation for certification bodies of Art. 43(2)(b) in conjunction with Art. 4 (5) GDPR) also include the certification criteria approved by the competent data protection supervisory authority or the Board.
2. The client's obligation to take the necessary precautions for evaluation and supervision in accordance with 4.1.2.2(c)(1) must also contain regulations (equivalent to the regulation for certification bodies of Art.42(2)(c) GDPR), which stipulate appropriate intervals for renewed evaluations or supervisions (regularity).
3. The client's obligation to allow full transparency to the competent supervisory authority with respect to the certification procedure including contractually confidential matters related to data protection compliance pursuant to Articles 42(7) and 58(1)(c).
4. The client's obligation to provide the certification body with all information and access to its processing activities which are necessary to conduct the certification procedure.
5. The client's obligation to comply with the GDPR and without prejudice a reference to the tasks and powers of the supervisory authorities competent under Article 42(5).
6. In addition to the minimum requirements mentioned in 4.1.2.2, the certification body shall be entitled to disclose all information necessary for the granting of certification in accordance with Articles 42(8), 43(5).
7. The client's obligation to take the necessary precautions for the investigation of complaints according to 4.1.2.2 (c)(2) and (j) must also contain (equivalent to the regulation for certification bodies of Art. 43(2)(d) GDPR) precise explanations on the structure and procedure of complaint management and these must be integrated into the management of the certification body.
8. In addition to the minimum requirements mentioned in 4.1.2.2, the consequences of the suspension or withdrawal of accreditation shall also be regulated in the agreement. The consequences of the withdrawal of the accreditation arise from point 4.3.1(c) of DIN EN ISO/IEC 17011:2017 and point M.8.3.2.1 of IAF/ILAC A5:11/2013. The withdrawal of an accreditation has consequences for the clients of the certification body. For this reason, the certification agreement shall indicate and stipulate that the certification of the client is dependent on the accreditation of the certification body. The suspension or withdrawal (termination or revocation) of the accreditation shall result in the invalidity of the certification. Appropriate procedures shall be integrated into the management of the certification body.

   In addition to the minimum requirements, mentioned in 4.1.2.2, the transfer of certifications in the case of termination of accreditation according to Art. 43 GDPR shall be regulated in the agreement.

   In the case of the termination or the renouncement, the DAkkS assesses whether the transfer of the certification takes place in accordance with the rules. This shall also be regulated in the agreement.

9. In addition to the minimum requirements, mentioned in 4.1.2.2, compliance with deadlines and procedures shall also be regulated. The certification agreement shall stipulate that deadlines and procedures resulting, for example from the certification scheme or other regulations, must be observed and adhered to.
10. In addition to the minimum requirements, mentioned in point 4.1.2.2 (k), an obligation to provide information in the event of changes in actual or legal circumstances must also be regulated. It is to be stipulated that clients have an obligation to inform the certification body in the event of significant changes in actual or legal circumstances and in its products, processes and services concerned by the certification. The certification body is obliged to determine the facts of the case within 4 weeks and to take appropriate measures, when made aware of such changes, which could have an impact on the compliance assessment statement.
11. In addition to point 4.1.2.2 of DIN EN ISO/IEC 17065, the expected duration of the process is agreed between the parties involved and defined contractually.

Regarding 4.2 Handling impartiality

According to 3.13 DIN EN ISO/IEC 17065, the certification body is only considered impartial if its independence and objectivity are guaranteed. Conflicts of interest shall not exist. Otherwise the execution of the activity is not possible.

The GDPR stipulates in Article 43(2)(a) and (e) separate provisions on demonstrating independence respectively the absence of conflicts of interest. The rules of DIN EN ISO/IEC DIN 17065 shall be supplemented as follows:

Regarding 4.2.1

Impartiality in this sense is only given, if the following additional requirements are met:

1. In accordance with Art. 43(2)(a) GDPR, separate evidence of the independence must be submitted to the competent data protection supervisory authority. This applies in particular to evidence of the financing of the certification body insofar as it relates to ensuring impartiality.
2. In accordance with Art. 43(2)(e) GDPR, the certification body must also have demonstrated to the competent data protection supervisory authority that its tasks and obligations do not lead to a conflict of interest. Such conflicts could arise, for example, from a high turnover dependency on clients or other economic pressure on the certification body.
3. In accordance with DIN EN ISO/IEC 17065, the certification body must also be a third party within the meaning of DIN EN ISO/IEC 17000:2005. A third party is a body which is independent, examines the subject-matter of certification and is independent of any interests as a user of the subject-matter of certification. Pursuant to Article R 17 para 3, first sentence, of Decision No 768/2008/EC, a certification body must be an independent third party, who is in no way affiliated with the entity it assesses. Paragraph 4 of Article R 17 provides that a certification body, its top management and the employees responsible for carrying out the conformity assessment tasks may not be the designer, manufacturer, supplier, installer, purchaser, owner, user or maintenance operators of the products under assessment nor may they be authorized representatives of one of these parties, unless this relationship does not call the impartiality of the parties into question, because it is of minor importance. Therefore, the necessary impartiality and the separation of the bodies involved must be ensured and documented. A body that concludes contracts with certification clients is not a third party. Consequently, in particular awarding bodies and contracting entities and their organizations, which are or may be contract partners, cannot themselves be certification bodies. If a legal separation of the certification body from such an organization was established, the following point applies.

Regarding 4.2.7

According to point 4.2.7 of DIN EN ISO/IEC 17065, the certification body shall ensure that activities of legally separated legal entities, with which the certification body, or the legal entity to which it belongs to, has relations, do not affect the impartiality of its certification activities. It has to be taken into consideration that any type of economic relation between the certification body and the legal entity, depending on its features, may affect the impartiality of its certification activities.
A certification body which belongs to or is controlled by a legal entity (e.g. an association or a public corporation), or has other ties to a legal entity, and whose members or shareholders are manufacturers, suppliers, processors, or controllers certified by this certification body, can only be regarded as an independent third party if it is independent pursuant to Art. 43(2)(a) GDPR, more specifically impartial pursuant to 3.13 of DIN EN ISO/IEC 17065 and proven to have no conflicts of interest. This may be the case if

1. the certification body is legally separated from the legal entity, and
2. the employees of the certification body and of the legal entity are separated and (the employees of the legal entity) do not work for the certification body in any way, particularly not in certification, testing and inspection procedures (see only 4.2.8 of DIN EN ISO/IEC 17065:2013); and
3. the top management of the certification body commits itself to impartiality in the shareholders' agreement or in the statutes of the certification body, according to item 4.2.5 of DIN EN ISO/IEC 17065, and
4. if the statutes of the certification body and/or the shareholders' agreement contain a clause on the autonomy of the managing director and/or the head of the certification body, and
5. in the substantiation of point 4.2.2 of DIN EN ISO/IEC 17065, there is no economic relation of dependence on the members of the legal person or the legal person itself.

Regarding 4.3 Liability and financing

In addition to the comments on liability and financing in 4.3, the requirements of 5.3.2 of DIN EN ISO/IEC 17021 shall also be observed:
The certification body must be able to demonstrate that it has assessed the risks arising from its certification activities and that it has appropriate measures at its disposal (e.g. insurance or reserves) to cover the liabilities arising from its activities in the geographical regions, in which it operates. The certification body shall demonstrate its financial stability and independence. The decision with respect to the selection and designation of the supporting documents lies within the discretion of the DAkkS and the responsible data protection supervisory authority. The certification body must have pecuniary damage liability insurance appropriate to the scope of its activities. The calculation of the necessary coverage shall be based on a risk assessment by the certification body.

Regarding 4.6 Publicly accessible information

Pursuant to 4.6(d), information concerning the handling of complaints and appeals shall be published by the certification body in accordance with Art. 43 (2)(d) GDPR. At the same time, this publication obligation does not only refer to individual incidents, but also to the structure and procedure for handling complaints by the certification body.

Pursuant to Art. 42(3) GDPR, in addition to 4.6(a) the information concerning the certification schemes used by the certification body, all versions of the certification procedures as well as the approved criteria in accordance with Art. 42(5) GDPR stating the authorized duration of applicationare to be published. The form of publication should be appropriate in order to inform the public as comprehensively as possible. This is usually guaranteed by the electronic form.

III. Chapter 5: Structural Requirements

According to 3.13 DIN EN ISO/IEC 17065, the impartiality of the certification body is only given, if its independence and objectivity are guaranteed. Additionally to Chapter 5.2 (Chapters 5.1.1 and 5.2) of DIN EN ISO/IEC 17065, the certification body must prove to the satisfaction of the competent data protection supervisory authority within the accreditation procedure that the mechanism to ensure independence meets the requirements of Art. 43(2)(a) and (e) GDPR and that their tasks and obligations do not lead to a conflict of interest. Independence means that the body in question can act completely free from instructions and pressure and that its financial stability is ensured.

IV. Chapter 6: Resource Requirements

In addition to Chapter 6 of DIN EN ISO/IEC 17065, in accordance with the GDPR, in order to be accredited as a certification body, the certification body must be able to demonstrate the following:

1. Appropriate expertise regarding data protection (Art. 43(1) GDPR)
2. Independence and expertise regarding the subject-matter of the certification (Art. 43(2) GDPR)

Regarding 6.1.2.1 Human resources competence

The certification body shall have and be able to demonstrate resources with relevant and appropriate knowledge in the following areas:

1. Knowledge of the relevant standards for conformity assessment (in particular ISO standards, laws, etc.)
2. Knowledge of the management systems relevant to the certification area (e.g. ISO 9001 /27001 /27017 /27018 / 27701/ IT-Security)
3. Knowledge of data protection law (GDPR/Federal Data Protection Act (BDSG)/relevant federal state data protection laws)
4. Knowledge of telecommunication law as well as the law of information society services respectively the ePrivacy Regulation
5. Where appropriate, knowledge of further relevant data protection standards, based on the certification schemes applied.

Furthermore, knowledge and experience in technical and organizational data protection must be ensured and demonstrated, in particular in the areas listed in Annex 3, as far as they are relevant for the certification scheme used.

The employees responsible for the evaluation and decision-making must have completed a relevant university degree recognized in the Federal Republic of Germany.

Both legal and technical expertise must be present within the responsible employees, but not necessarily within one person.

Specifically, the following conditions must be fulfilled and demonstrated:

Technically: (No. 2 or No. 3 must be fulfilled in addition to No. 1):

1. At least one degree in accordance with EQF2[2] at a German state or state-recognized higher education institution which is predominantly characterized by the subjects of computer science, technology, mathematics or a subject comprisesing corresponding IT examinations or if the competent authority has conferred the right to make use of the designation "engineer".
2. For decision-makers, a degree according to EQF2 level 6[3] (e.g. Bachelor) requires at least five years of professional experience, and a degree according to EQF2 level 7[4] (e.g. Master) requires at least four years of professional experience in technical data

[2] EQF2 – European Qualifications Framework

[3] Level 6 - first cycle (Bachelor's or equivalent degrees according to the European Qualifications Framework), with advanced knowledge in a field of work or learning, demonstrating mastery of the subject and capacity for innovation, and necessary to solve complex and unforeseeable problems in a specialised field of work or learning, based on a critical understanding of theories and principles.

[4] Level 7 - second cycle (Master's or equivalent degrees according to the European Qualifications Framework), with highly specialised knowledge, specialised problem-solving skills, as a basis for innovative thinking, to acquire new knowledge and develop new processes and to integrate knowledge from different fields.

protection with focus on more general and comprehensive expertise and professional experience in data protection.

3. For evaluators, a degree according to EQF2 level 6 (e.g. Bachelor) requires at least five years of professional experience, a degree according to EQF2 level 7 (e.g. Master) requires at least three years of professional experience in technical data protection and knowledge and experience in the testing procedure (e.g. certifications/audits).

Legally: (No. 2 or No. 3 must be fulfilled in addition to No. 1):

1. The legal competence is acknowledged to individuals, who have studied law at a German state or state-recognized university for at least eight semesters and have obtained the academic degree Master (LL.M.) or who have passed the 1st Legal State Examination.
2. Decision-makers must have at least four years of professional experience in data protection law with focus on more general and comprehensive expertise and professional experience in data protection.
3. Evaluators must have at least three years of professional experience in data protection law as well as knowledge and experience in the audit procedures (e.g. certifications/audits).

In order to be able to assess the competence of the body to be accredited, the accreditation procedure is accompanied by an on-site inspection (witnessing model/see Annex 2) in addition to reviewing the documents submitted in writing.

The employees in charge of evaluation and decision-making must keep their knowledge on the procedures and relevant information up to date. Proof of knowledge can be demonstrated by training certificates, relevant work experience (e.g. certification procedures carried out) or in other ways the competent data protection supervisory authority deems satisfactory for the accreditation procedure respectively the surveillance assessments of the accredited certification body.

The assessment of the equivalence of foreign qualifications shall be based on the documentation referred to in Directive 2013/55/EU concerning the recognition of professional qualifications (OJ L 354, 28.12.2013, p. 132-170) in conjunction with Directive 2006/100/EC of 20.11.2006.

Regarding 6.2.2

If evaluation activities are outsourced to external bodies, those bodies shall be subject to the same conditions as the certification body. In particular, these data protection-specific requirements have to be observed by the subcontracted body.

V. Chapter 7: Process Requirements

Regarding 7.1 General information

The certification criteria are part of the certification scheme.

The authorized certification scheme shall include the planned evaluation methods (see 7.4). Reference here for is made to chapter 3.9 of DIN EN ISO/IEC 17065.

Regarding 7.1.2

The competent supervisory authority shall be notified before a certification body starts operating an approved European Data Protection Seal in a new Member State from a satellite office.

Regarding 7.2 Application

In addition to point 7.2 of DIN EN ISO/IEC 17065, the client must describe the subject-matter of certification in detail within the application. This also includes the presentation of interfaces and more specifically the transitions to other systems and organisations. In doing so, underlying protocols as well as other guarantees are to be provided. If processors are used to execute the data processing operations of the subject-matter of certification, they shall be named in the application including their adopted responsibilities and associated tasks, and the relevant (joint) controller/processor contract(s) shall be attached to the application.

Regarding 7.3 Evaluation of applications

In addition to point 7.3 of DIN EN ISO/IEC 17065, the planned evaluation methods shall be contractually stipulated in the certification agreement between the applicant and the certification body taking into account the data protection law applicable to the client.

The monitoring of contracts under 4.1.2.2 shall be part of the management of the certification body.

The period between the completion of the last evaluation and the certification decision may only exceed 3 months in justifiable exceptional cases.

In addition to point 7.3.3 of DIN EN ISO/IEC 17065, the certification body shall demonstrate that appropriate technical and legal competences (e. g. in the field of data protection) exist for the certification activities of the individual case, despite a lack of experience with either, the subject-matter of certification, the scope of application or the type of client.

Regarding 7.4 Evaluation

The certification body shall ensure that mechanisms used for granting certification describe sufficient evaluation methods for assessing the compliance of the processing operation(s) with the certification criteria. These methods and the findings of the evaluation shall be documented in detail.

In addition to point 7.4.1 of DIN EN ISO/IEC 17065, the evaluation methods laid down in the certification scheme are implemented by the certification body within the framework of the certification.

The appropriate evaluation methods particularly have to cover the following areas:

1. a method for assessing the necessity and proportionality of processing activities in relation to their purpose and where applicable in relation to the data subject concerned,
2. a method for assessing the composition and evaluation of all risks considered by the controller and, if applicable the processor, with regard to Art. 5 GDPR and the legal consequences according to Art. 30, 32, 35 and 36 GDPR and the determination of technical and organizational measures according to Art. 24, 25 and 32 GDPR, insofar as the specified legal standards apply to the subject-matter of certification, and
3. a method for evaluating remedies, including guarantees, safeguards and procedures, to ensure the protection of personal data in the context of the processing operations forming part of the subject-matter of the certification as well as the demonstration that the legal requirements are being met.

The certification body shall ensure that these evaluation methods are validated. Meaning, comparable evaluation methods are also used in comparable procedures and lead to comparable results. Verification of this is to be submitted to the accreditation body within the assessment of the certification scheme.

In addition to point 7.4.4 of DIN EN ISO/IEC 17065, the evaluation may be carried out by external evaluators previously recognized by the certification body as competent.

The legal and factual relationships of these external evaluators towards the certification body are governed by the provisions of Chapter 6 of DIN EN ISO/IEC 17065, taking into account the aforementioned provisions.

In addition to point 7.4.3 of DIN EN ISO/IEC 17065, the certification body may request further information and/or documentation, it considers necessary for certification during the certification procedure. The certification body has the right to terminate the certification procedure in case the applicant does not comply with the obligation to provide the requested information and/or documentation.

In addition to point 7.4.5 of DIN EN ISO/IEC 17065, the certification body shall define the significance of other certifications hold by the client (e.g. IT-Security, DIN EN ISO/IEC 27001/27002). Certifications which can be considered for evaluation, how and to what extent they can be considered for evaluation shall be described as well as the concrete effects this has on the remaining scope of the evaluation and on the evaluation methods. According to 7.4.5 these evaluations must be completed before the client submits an application and must have been carried out by a conformity assessment body which fulfills the requirements for equivalence according to paragraph 6.2.2.1 DIN EN ISO/IEC 17065.

Existing certifications may particularly be taken into account as follows:

1. A data protection certification in accordance with Art. 42 GDPR, where parts of the subject-matter for certification have already been certified by an accredited certification body, can be considered as a partial evaluation.
2. However, data protection certifications according to Art. 42 GDPR are not acceptable to completely replace (partial) evaluations. The certification body continues to be obliged to check the current compliance with the requirements (of the submitted certification), at least randomly, and to evaluate existing certifications. Effects on the period of validity of the certification submitted do not result.
3. Other certifications, granted by an accredited certification body, as such according to Art. 42 DSGVO (e.g. ISO certifications) can also be considered as a factor for conformity and may be considered within the framework of certification. They are, however, not sufficient to completely replace (partial) evaluations. Here, too, the certification body is obliged to monitor compliance with the requirements by means of the verification of the audit report at least randomly and to evaluate the adequacy of the existing certifications.
4. The time limitation of the certificates to be considered shall be documented and kept available according to 7.7 (resp. 7.7.2).

Such compliance requires the availability of a full certification assessment or information, enabling an assessment of the certification activity and results. A certificate of certification or similar attestations of certification are herefor not sufficient. If deviations from the requirements or other irregularities result from such an audit, then the evaluation shall be extended within the framework of the ongoing certification procedure and, if necessary, on the entire subject matter already certified.

In addition to Point 7.4.6 of DIN EN ISO/IEC 17065, the certification body shall state in detail, how the client is to be informed about deviations resulting from a certification program, as required in Point 7.4.6, in its certification criteria. At the very least, the form and timing of the provision of such information shall be defined.

In addition to point 7.4.9 of DIN EN ISO/IEC 17065, the certification body shall describe, how this type of documentation is performed. The form and content of the documentation must be designed in such a way, that both the evaluation as such and the subsequent evaluation results are comprehensive and plausible.

The documentation shall be fully accessible during the accreditation procedure and at any time upon request of the data protection supervisory authority.

Regarding 7.5 Review

In addition to point 7.5.1 of DIN EN ISO/IEC 17065, the certification body shall demonstrate - within the certification scheme and within the management system referred to in point 8.1 of DIN EN ISO/IEC 17065 - how the person(s) tasked with the assessment have neither directly nor indirectly been involved in the evaluation process. The application of these criteria and their results shall be documented within the framework of the assessment.

Regarding 7.6 Certification decision

According to paragraph 7.8 DIN EN ISO/IEC 17065, the certification body must publish a short public assessment of the certification result.

The certification body shall inform the competent data protection supervisory authority of the certification in writing at least one week before the certification is granted. The written information must include the name of the client, the description of the subject-matter of the certification and a short public assessment.

In addition to point 7.6.1 of DIN EN ISO/IEC 17065, the certification body shall state in detail, how its independence and responsibility towards the certification decisions are ensured.

In addition to point 7.6.2 of DIN EN ISO/IEC 17065, the decision on certification must be held by the head of the certification body or a qualified person directly appointed by him or her. DIN EN ISO/IEC 17065 para. 7.6.3 must be observed. The evaluation may be carried out by experts, previously recognized by the certification body, as described in addition to 7.4.2.

In addition to point 7.6.6 of DIN EN ISO/IEC 17065, the certification body shall state, how the client will be informed about the decision not to grant the certification. Further, it must also state which options the client has in order to appeal the decision of the certification body in the above mentioned cases and what form and deadline the client must adhere to.

Regarding 7.7 Certification documentation

In addition to point 7.7.1. e) of DIN EN ISO/IEC 17065 and in accordance with Art 42(7) GDPR, the period of validity of certifications shall be limited to a maximum of three years.

In addition to point 7.7.1. e) of DIN EN ISO/IEC 17065, the time period of the intended surveillance as defined in Chapter 7.9 shall also be documented.

In addition to point 7.7.1 f) of DIN EN ISO/IEC 17065, the certification body shall inform the client as part of the certification documentation about the subject-matter of the certification (if applicable, stating the version or identification number).

Regarding 7.8 Directory of certified products, processes and services

In addition to point 7.8 of DIN EN ISO/IEC 17065, the certification body must keep the information containing certified products, processes and services internally available and generally accessible via the Internet. The information to be kept internally and the public directory must in addition to point 7.8 of DIN EN ISO/IEC 17065 contain:

A short assessment regarding the respective certification result,

1. from which the exact subject matter of certification (including version or function status) is derived,
2. the audit procedure (including the underlying criteria of the certification of (with version if applicable)) and
3. to derive the audit result.

Additionally, the directory must include

1. Contact details of the applicant (legal or natural person),
2. a registration number,
3. the date of certification and the expiry date of the certification,
4. Information about the initial or re-certification,
5. information on possible surveillance activities to maintain certification, as well as
6. the possible involvement of external evaluators.

In addition to point 7.8 of DIN EN ISO/IEC 17065 and point 8.3 of DIN EN ISO/IEC 17021, and pursuant to Art. 43(5) GDPR, the certification bodies shall inform the competent data protection supervisory authorities of the reasons for granting or revoking the applied for certification.

Regarding 7.9 Surveillance

In addition to items 7.9.1, 7.9.2, 7.9.3 and 7.9.4 of DIN EN ISO/IEC 17065, 8.3 of DIN EN ISO/IEC 17021 and pursuant to Art. 43(2)(c) GDPR, surveillance measures are required to maintain certification during the surveillance period.

Surveillance shall be performed at least two times during the certification cycle. These systematically repeated conformity assessment activities as a rule include the following types of inspection:

1. Regular warrantless surveillance, including site inspections,
2. Surveillance corresponding to the result of a risk analysis, including site inspections.

The regularity of warrantless surveillance shall be determined in the certification scheme. Furthermore, the type of surveillance must be defined and the way in which typical data protection risks are appropriately dealt with must be determined.

Warranted surveillance occurs in the event of anomalies, causing concern of a non-compliance with the certification requirements. The procedure and the necessary certification agreement with the client must be demonstrated at all times during the accreditation procedure and upon request by the data protection supervisory authorities.

Regarding 7.10 Changes affecting certification

In addition to points 7.10.1 and 7.10.2 of DIN EN ISO/IEC 17065, the certification body shall define processes in its certification scheme which ensure that the client is provided, in a timely manner, with general information on changes that might affect him. These changes derive from amendments to the law, the enactment of delegated acts of the European Commission, documents adopted by the European Data Protection Board, court rulings, as well as further

developments of the state of the art technology (as far as relevant for the future certification and surveillance). This must be included in the management system as defined in Chapter 8.

In addition to point 7.10.1 of DIN EN ISO/IEC 17065, the certification body shall define in its certification scheme,

1. which changes require a notification and, if applicable, an adjustment for the client,
2. which evaluation methods are to be performed by the certification body in such a case, and
3. what deadlines for the implementation of the measures exist, in order to maintain the existing certification.

Beyond that, the certification body shall define how it ensures that comparable audits are conducted in comparable certification procedures (even if the certification requirements change).

Furthermore the certification body shall also define which measures and processes are to be taken if the audit leads to the conclusion that the certification cannot be maintained. The appropriate measures and corresponding processes shall be implemented and kept available by the management of the certification body.

In addition to point 7.10.2 of DIN EN ISO/IEC 17065, the certification body shall define in its certification scheme in what cases and in what way the client is to provide the certification body with information (in case of changes initiated by the client). This is always the case, at least when changes have occurred in the subject-matter of the certification with regard to the processing of personal data, changes in the operational environment and/or changes in the application context or changes in other framework conditions that are relevant for the certification statement. This applies in particular to changes in pertinent legal standards concerning the subject-matter of certification as well as to the changes in the state of the art technology that have been determined by the client. In this case, any measures initiated by the notification must be defined by the certification body and by the client. The certification body shall also define how to ensure that comparable measures are taken in comparable cases. Furthermore, the appropriate measures and corresponding processes shall be implemented and kept available by the management of the certification body.

Regarding 7.11 Termination, reduction, suspension or withdrawal of certification

In addition to Chapter 7.11.1 of DIN EN ISO/IEC 17065, the competent data protection supervisory authority must be immediately informed in writing of any measures taken and of any continuation, restriction, suspension or withdrawal of the certification.

Furthermore, in cases where the certification body determines non-compliance it must define in which measures are to take place, and which cases (of non-compliance) constitute measures in the first place.

The certification body is obliged to observe and accept the powers of the competent supervisory authority laid down in Art. 58 (2) (h) GDPR and to withdraw or not issue certification to an applicant if the conditions for certification are not or are no longer fulfilled.

Regarding 7.12. Documentation

All documentation of the certification body must be complete, verifiable, up-to-date and auditable. This applies both to completed certification procedures without a positive outcome and to ongoing certification procedures. In ongoing certification procedures, certification criteria which is fulfilled and not fulfilled must be distinctly evident. In addition to that, the certification body must keep statistics on completed and terminated procedures.

In addition to Chapter 7.12.1, all records concerning the certification process shall be retained for a further three years, beyond the period of validity of the certification and beyond the completion of the certification agreement. In the event of disputes between the certification body and the client or the client and the competent supervisory authority, this period may be extended beyond the period of validity of the certification until the conclusion of this procedure.

Regarding 7.13 Complaints and appeals

In addition to point 7.13.1 of DIN EN ISO/IEC 17065, the certification body shall define,

1. who can file complaints or appeals,
2. who from the certification body is in charge of processing complaints or appeals,
3. what type of inspections are to take place in this context, and
4. what possibilities of revision exist for the parties of the complaint or appeal.

Furthermore, the certification body must define deadlines for the parties involved, in order to control time limits on the process of handling complaints and appeals.

In addition to point 7.13.2 of DIN EN ISO/IEC 17065, the certification body shall define,

1. how and towards whom this confirmation is to be submitted,
2. what deadlines apply for this and
3. what processes are to be initiated subsequently.

In addition to point 7.13.1 of DIN EN ISO/IEC 17065, the certification body shall define, how the separation of employees between certification activities and the handling of objections and complaints is to be ensured. According to point 7.13.5 of DIN EN ISO/IEC 17065, the decision resolving the complaint or appeal must be made, evaluated and approved by persons who are not involved in the certification activities related to the complaint or objection.

VI. Chapter 8: Management System Requirements

General Remarks

The general prerequisite of the management system pursuant to Chapter 8 of DIN EN ISO/IEC 17065 is that the implementation of all requirements from the previous chapters is documented, evaluated, controlled and independently supervised by the accredited certification body in the context of the application of the certification mechanism.

The basic principle of a management is to specify a system according to which the set goals - here: Implementation of the certification services – are to be effectively and efficiently achieved through appropriate stipulations. This requires the transparency and auditability of performed implementations of the accreditation requirements by the certification body and its permanent maintenance.

To this end, the management system must stipulate a method for how these requirements can be achieved in compliance with the data protection regulation, supervised, and continuously audited by the accredited body itself.

These management principles and its documented implementation must be transparent and disclosed by the accredited certification body,

1. during the accreditation procedure, and
2. thereafter at any time upon request of the data protection supervisory authority, e.g. during an investigation in the form of data protection reviews (Art. 58(1)(b) GDPR),
3. or a review of the certifications granted in accordance with Art. 42(7) GDPR (Art. 58(1)(c) GDPR).

In particular, the accredited certification body must permanently and continuously make public:

1. What certifications have been carried out.
2. On what basis (or certification schemes) the certifications were carried out.
3. Under which conditions (recital 100) the certification is valid, and.
4. how long the certifications then remain valid.

Detailed Amendments:

Regarding 8.1 General information

The amendments from this document must also be applied to both Option A and Option B. In both cases, but especially when Option B is applied, it must be ensured that the application of the amendments is explicitly tailored to the scope of application so that the amendments are identifiable and verifiable. The reference to the application of the amendments must be verifiable.

Regarding 8.1.1:

For example, processes according to the previous chapter must be implemented in the certification body's own management. This includes:

1. Management of certification criteria and corresponding authorization procedures
2. Inspection, control, evaluation and improvement of the structure of the internal processes of the certification body with continuing corresponding internal documentation,
3. Handling of the complaint management,
4. Suspension and withdrawal of certification and documentation of reasons therefor,
5. Contract management,

6. Ensuring independence (impartiality/financial stability) and the management of the corresponding verifications,
7. Publication of certification criteria/certification decisions etc.,
8. Resources (personnel competence and external resources),
9. Application management,
10. Supervision of changes that affect certifications and
11. Supervision of the application of certifications.

In addition to Chapter 8 of ISO 17065, the following additional points must be implemented:

8.9 Continuation of the evaluation methods

8.9.1 The certification body shall establish procedures in order to guide the continuation of the evaluation methods for the application of the evaluation in point 7.4. Updating is to take place in the course of changes to the legal framework, the relevant sources of risk, the state of the art technology and the implementation costs of technical and organizational measures.

8.9.2 The procedures shall establish the necessary guidance procedures to ensure that:

1. any relevant changes to the legal framework (pursuant to point 7.4 and the corresponding amendments in this text) are,
2. components of the contract between the client and the certification body are,
3. all relevant and newly emerging (categories of) sources of risk, deficiencies in information technology, devices and safety technology, and
4. the progress in the state of the art technology concerning processing activities and technical and organizational measures that can be used to grantee compliance with the legal requirements (especially considering the implementation of data protection principles and the security of processing) are

recorded, documented, evaluated and depicted in the evaluation methods.

In addition, the management system must be able to ensure that changes in requirements for catalogues of criteria and certification procedures by the data protection supervisory authorities and the data protection board are supervised, and that these changes are immediately integrated into the certification body's own procedures. The accreditation body and the competent data protection supervisory authority shall be informed of the changes.

The certification body must also ensure that legal acts or rather other requirements by the data protection board or data protection supervisory authorities are promptly recognized and immediately implemented. The accreditation body and the competent data protection supervisory authorities shall be informed about the changed implementations.

8.10 Perpetuation of expertise

Certification bodies shall establish procedures for the guidance of continued education, under consideration of the developments listed in point 8.9.2., in order to keep the expertise of their employees up to date.

8.11 Accountabilities and responsibilities

8.11.1 Relationship between certification body and its clients

The following points shall be established for the implementation of pertinent procedures and appropriate communication structures between the certification body and clients:

1. Maintenance of a business allocation plan of the accredited certification body, in order to

a. requests information, or
b. enable contact in the event of a complaint regarding the issued certification.

2. Maintaining the application process, including:
    a. the status of an application assessment for a submitted application for certification
    b. an assessment by the competent data protection supervisory authority
        i. a response from the competent data protection supervisory authority (with current date)
        ii. a decisions of the competent data protection supervisory authority (with current date).

8.11.2 Conformity assessment activities and their procedures

The focus must be on conformity assessment activities and their procedures. This includes

1. Disclosure of conformity assessment activities so that changes or rather the process of changes can be comprehended; therein is to be recorded:
    a. on what basis a conformity program was created, if necessary with respective references, e.g. the technical norms DIN EN ISO/IEC 17000 and DIN EN ISO/IEC 17011 and additional sources, such as special laws and likewise specific technical norms, which are employed depending on the application;
    b. the employment of, if applicable, specific methods in the concepts and procedures of the audit for the conformity assessment so that included standards for the target/actual comparison are achieved, controlled and continuously tested and improved;
    c. the documentation of inspections, audits and improvements of the standards, including the exact time and reasons for the respective adjustment (as specified in point 7.10).
2. Inspections of conformity assessment (by a third body, delegation of tasks within the certification process)
3. Documentation and inspection of the duty of impartiality (pursuant to point 4.2.3)
4. Accounts for changes in the documentation and processes as part of publication management; i.e. as consequences from the implementation of points 4.1.2.2, 4.6 and 7.8.
    a. out of certification schemes;
    b. out of standards for conformity assessment in certification schemes
    c. from the minimum requirements of the certification agreements
5. Supervision of the specific certifications and their respective publications (pursuant to point 7.8) and, if applicable according to point 4.6., specific complaints concerning a certification.

8.11.3 Complaint management

A complaint management system shall be established as an integral part of the management system; which shall in particular realize the requirements of points 4.1.2.2(c), 4.1.2.2(j), 4.6(d) and 7.13 DIN EN ISO/IEC 17065.
Resulting consequences are that

1. Due to major changes, a new risk assessment must follow.
2. This kind of risk assessment can have a direct influence on the implemented subject-matter of certification.

In the event of substantiated complaints, the competent data protection supervisory authority must be informed.

8.12 Further procedures

The procedures for the event of suspension or withdrawal (termination or appeal) of accreditation shall be integrated into the management system of the certification body. This includes procedures for the handling of the associated certifications.

If the certification body is instructed by the data protection supervisory authority to appeal an approved certification or not to approve a certification, in accordance with Art. 58(2)(h) GDPR, the certification body must ensure within its management system that the respective client is informed about the order and its resulting consequences. It must further adjust the corresponding entry in the register and inform the data protection supervisory authority about the adjustment.

Appendix 1 List of Abbreviations / Glossary

Unless the context indicates otherwise, the following definitions shall apply:

Requirements	Describes the data protection specific amendments to the legal and normative requirements for accreditation according to VO (EG) 765/2008 in connection with DIN EN ISO/IEC 17065 according to Art. 43 para. 1 lit. b GDPR
Accreditation	Accreditation is the confirmation by a national accreditation body that a certification body meets the requirements stipulated in standards and, where appropriate, in additional requirements, including those in relevant sectoral accreditation schemes, in order to perform a specific conformity assessment activity.
Accreditation Committee (AKA)	The AKA is an internal procedural decision-making body within the DAkkS that makes accreditation decisions based on the assessment results and further findings (administrative act). The AKA consists of three members. Two members are appointed by the data protection authorities. A positive accreditation decision can only occur unanimously. A single negative vote suffices for a negative decision.
AKA members	AKA members are technical experts, who may contribute to accreditation decisions and who have not been involved in the evaluation to which the AKA is to make a decision in the concrete procedure.
Assessor	The assessor is a technical expert, who performs assessments within the accreditation.
Client	A controller or processor submits his or her implemented processing to the certification procedure (Art. 42 Para. 6 S. 1 GDPR).
Certification Scheme	A certification scheme is a document issued by a certification body or by an independent private or public scheme owner that describes the specific requirements and rules as well as the inspection procedures - which need to be applied to the conformity assessment of the product, process, service, system or person – in order to declare the assertion connected to the

	conformity assessment verification (e.g. laboratory result, analysis, inspection report, trial, certification, etc.) systematically and scientifically plausible.
(Approved) Criteria	Authorized certification criteria within the meaning of the GDPR are criteria that have been approved by the data protection supervisory authority pursuant to Art. 57(1) GDPR as part of the certification scheme, previously determined eligible by the DAkkS in accordance with 4.6.3.
Scheme Owner	owns the rights to and supervises the certification scheme.
Certification Mechanism	equates to the certification scheme and its management.
Certification Body	equates to the conformity body as a third party that operates a certification scheme.
Certification activities	All activities by a certification body according to DIN EN ISO/IEC 17065.

Appendix 2: Witnessing Model

Witnessing (performed by employees of the data protection supervisory authority or by the authorized representative and the accreditation body) principally takes place at the site where the activity within the certification process is carried out. Generally this is at the client or its processor of the certification body; depending on the certification scheme, but can also be concluded in the premises of the certification body or at other locations in which activities pertaining to the evaluation are conducted. The DAkkS (in coordination with the responsible data protection supervisory authority) reserves the right to determine what employees must undergo Witnessing and for which activities in the process of certification. The scope of the required Witnessing within the evaluation procedure is to be determined by the DAkkS (in coordination with the responsible data protection supervisory authority) according to the following principles:

1. For the initial accreditation, a certification body must at a minimum conduct one witness audit per application of the certification scheme;
2. It is permissible to make up for outstanding witness audits within an appropriate period of time in accordance to ISO 17011 and to grant the accreditation under the condition that the outstanding witness audit is conducted,
3. in the subsequent supervision of the accreditation pursuant to ISO 17011, a witness audit must be conducted for at least one component out of all scheme of the certification body; within the accreditation cycle, at least 50% of all components out of all schemes must be covered by a witness audit,
4. Witness audits may, depending on further assessments and risk-oriented considerations, be mandated unscheduled at any time.

The amount of witness audits may be decreased if the accreditation body can justify the adequate confidence in the activity of the certification body. If the certification body wants to employ a new certification scheme, a new Witnessing is required.

Annex 3: Knowledge and Experience in Technical and Organizational Data Protection

1. Applied cryptography (e.g. encryption methods, hash methods, PKI)
2. Pseudonymisation/Anonymisation
3. Privacy Enhancing Technologies (PETs)
4. Identity management and role-based access control based on a well-defined concept
5. Logging and transparency
6. Risk-based approach according to GDPR (e.g. Article 5(1) GDPR and corresponding ISO standards)
7. Procedure for conducting a data protection impact assessment (e.g. Standard Data Protection Model, ISO 29134)
8. Information and cyber security (with regard to the rights and freedoms of natural persons)
9. Data protection by design / data protection by default
10. Process for deleting personal data / deletion concepts
11. Data protection management systems and governance