Requirements for Data Protection Certification Schemes

Data protection examination criteria, systems and methods for the adaptation and application of technical standard DIN EN ISO/IEC 17067 (scheme type 6)

Version 3.0 (17 November 2025)

Contents

1 Objective and integration into regulatory framework

1.1 Objective

In order to prepare for accreditation, the certification body or scheme owner must create a certification scheme and ask the German Accreditation Body (DAkkS[1]) to check its suitability in accordance with DIN EN ISO/IEC 17011 (cf. DAkkS Rule 71 SD 0016). The certification scheme will essentially revolve around certification criteria for the implementation of data protection requirements. The relevant criteria will either be approved by the competent data protection supervisory authority in accordance with point (n) of Art. 57 (1) of the General Data Protection Regulation (GDPR) in conjunction with Art. 42 (5) GDPR[2], or they will be sent to the European Data Protection Board (EDPB) for approval (usually by the competent supervisory authority) in accordance with Art. 63 and point (c) of Art. 64 (1).

This document describes the minimum requirements for the certification criteria which, in addition to the specifications of DIN EN ISO/IEC 17067, must be met by all certification schemes. There may also be additional requirements due to the specific nature of a certain certification scheme.

In summary, each certification scheme must satisfy the following mandatory requirements:

(1) the specifications of DIN EN ISO/IEC 17067 (scheme type 6);

(2) the minimum requirements for all certification schemes, as described in this document; and

(3) if necessary, specific requirements, which may, for example, arise from a certification scheme being tailored to a specific field or addressing a specific form of personal data processing, or because potential subjects of certification fall within the scope of specific legal regulations.

---

1 Deutsche Akkreditierungsstelle GmbH (DAkkS) has its legal basis in the German Accreditation Body Act (AkkStelleG) in accordance with Regulation (EC) No. 765/2008.

2 When articles of the GDPR are referenced in the rest of this document, “GDPR” will be omitted from the citation.

Additional requirements may be stipulated by accreditation bodies, specifically taking into account the guidelines of the EDPB[3], the decisions adopted by the Independent Data Protection Supervisory Authorities of the Federation and the Länder (DSK), case law or accreditation practice.

For the reasons mentioned above, this document does not claim to be complete. The aim is to provide both a uniform basis for the German supervisory authorities to evaluate certification schemes and a guide for scheme owners and certification bodies to create their documents.

1.2 Integration into regulatory framework

When it comes to designing certification schemes, the starting point is DIN EN ISO/IEC 17067[4].

As DIN EN ISO/IEC 17067 is generic in nature, the independent supervisory authorities will make adjustments and additions to the standard to establish requirements specifically related to data protection criteria in accordance with Art. 42 (5).

DIN EN ISO/IEC 17067 contains a definition of different scheme types. Certification schemes for data protection seals have to be aligned with scheme type 6 in accordance with Art. 42 because of the professional practice of the competent supervisory authorities and the service nature of the subjects of certification.

1.3 Examination process

Each certification scheme must include an examination process that allows for a practical verification, a technical evaluation and a legal assessment to determine whether

3 Cf. “Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation” https://edpb.europa.eu/our-work-tools/our-documents/leitlinien/guidelines-12018-certification-and-identifying-certification_de.

4 In the application of the technical standards, DIN EN ISO/IEC 17067 is the follow-up standard to DIN EN ISO/IEC 17065, which is stipulated for use in point (b) of Art. 43 (1).

the applicant is meeting the relevant requirements on an ongoing basis. If a verification, evaluation or assessment reveals a need for change, appropriate measures must be taken as required. The examination process must be in place at the time of certification; it must be maintained and guaranteed for as long as the certification remains valid.

Each certification scheme must present the certification requirements, as listed in Section 1.1, and the methods used by the accredited certification body to examine the subject of certification.

The data protection examination method must be suitable for determining and documenting whether the applicant is properly satisfying the relevant data protection requirements and whether the applicant has implemented effective technical and organisational measures for the subject of certification in relation to the established and approved criteria pursuant to Art. 42 (5). The applicant will be deemed GDPR-compliant if such evidence is presented for the subject of certification.

All certification schemes must aim to ensure that certifications that have been issued properly are not subsequently challenged by an independent supervisory authority following a data protection audit. With this in mind, a certification scheme must be suitable for fully checking and documenting whether the subject of certification complies with the GDPR. The supervisory authority may exercise its supervisory powers at any time, and its audits may reveal that a certain form of data processing is actually unlawful.

1.4 Underlying documents

This document, which can be used to define criteria pursuant to Art. 42 (5) alongside the associated examination system and examination methods in conjunction with DIN EN ISO/IEC 17067 (scheme type 6), is based on

- the specifications of Art. 43;
- the EDPB guidelines mentioned above and other more specific EDPB guidelines;

- the ISO/IEC 17065 and ISO/IEC 17067 standards; and
- the DSK supplementary paper[5] pursuant to Art. 43 (3) in conjunction with DIN EN ISO/IEC 17065 for certification bodies that are to be audited as part of the DAkkS accreditation process in agreement with the competent and independent supervisory authorities.

5 "Accreditation requirements pursuant to Art. 43 in conjunction with DIN EN ISO/IEC 17065", available (in German) here: https://www.datenschutzkonferenz-online.de/media/ah/20201008_din17065_Ergaenzungen_deutsch_nach_opinion.pdf.

2 Certification criteria and requirements

2.1 General requirements

2.1.1 Description of the subject of certification

Each certification scheme must specify the processing activities for which it is to be used (i.e. the scope of the certification scheme). The scope of each certification scheme should be limited to processing that falls within the material and geographical scope of the GDPR.[6]

The minimum requirements for certification schemes, as set out in Section 2.1.3 and 2.2 ff. below, must be taken into account. The requirements must be checked by the accredited certification body and the competent data protection supervisory authority. If it is a generic certification scheme, the requirements specifically related to data protection must be detailed prior to certification, and the certification body must make sure that the relevant requirements are complete. Every certification scheme must state that the certification of a controller's processing activities will extend to any such processing performed by the controller itself – or by joint controllers – and by any processors that may be involved, including any sub-processors.

2.1.2 Information to be provided by the applicant regarding the subject of certification

Each certification scheme should contain specifications as to which information the applicant has to provide about the processing that is to be certified (i.e. the subject of certification) before the examination process can begin. The following information – if applicable to the processing in question – are required as a bare minimum:

6 Please note: The controller / processor does not have to fall within the geographical scope of the GDPR, as stipulated in Art. 42 (2). The scope of Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA ("JHA Directive") is not taken into account here, for example, as conformity with the JHA Directive cannot be the subject of certification under Art. 42.

1. the processing operations covered by the subject of certification;
2. the purpose of the processing operations and why the processing operations are necessary to achieve the purpose;
3. the recipients or categories of recipients;
4. the data processed in connection with the subject of certification; and
    a. which of that data can be defined as “special categories of personal data” pursuant to Art. 9;
    b. which of that data relates to criminal convictions and offences pursuant to Art. 10;
    c. which of that data relates to children in the sense of the GDPR;
5. whether someone is acting as a “processor”, as defined in Art. 8 No. 4, and, if so, for which processing operations covered by the subject of certification;
6. whether there are any “joint controllers” for certain processing operations covered by the subject of certification pursuant to Art. 26;
7. a stage-by-stage presentation of the entire processing chain, including the relevant controllers, and the respective actor and role model (actors, roles, relationships) for each stage of processing[7];
8. whether the processing operations involve the transfer of personal data
    a. outside the European Union or European Economic Area; or
    b. to international organisations.

7 This can either be done graphically, e.g. using standardised formats such as Business Process Modelling (BPM) or Unified Modelling Language (UML), or in text form.

Any such data transfers may also be carried out for the purposes of administration, maintenance, care or support to ensure that the subject of certification remains fully functional during the certification validity period. Any further transfers by processors must also be examined.

9. What are the main components and sub-components and how are they broken down (see processing operations using systems and services), e.g. by the following points:

   a. list of all participants or groups of participants (e.g. customers, users, administrators[8]);

   b. presentation of how data flows between components and participants are recorded, specifying the categories of data concerned;

   c. consideration and, if necessary, explanation of legal grounds for the processing of personal data in (sub-)components and for transfers in the case of data flows and types of data.

The connection between the relevant legal basis, the technical standards and the subject of certification depending on the specific scope of application must be clearly presented in each certification scheme.

It is also a good idea to list the points in the certification scheme where the relevant requirements of DIN ISO 17065, 17067 and the DSK supplementary papers are met (this can be done in the form of a matrix, for example).

2.1.3 Compliance with the relevant data protection requirements

In accordance with Art. 42 (1), certification procedures should serve as evidence that controllers and processors are complying with the GDPR in their processing operations. In order to achieve this goal, the certification criteria must guarantee compliance with all relevant requirements of the GDPR.

8 - footnote intentionally left blank -

The EDPB Guidelines 1/2018 on certification and identifying certification criteria[9] serve as a guide in this context, specifying aspects to be taken into account in each certification scheme. As this paper is under constant development, the articles of the GDPR listed in the following sections will be examined with varying degrees of detail. This does not reflect the importance of each article; it is for illustrative purposes only.

The information presented in tables in the following sections is not exhaustive, as further assessment techniques may be employed in addition to the examination methods listed there. The examination methods should be based on those defined in the standards, e.g. audits (ISO 17021), testing (ISO 17025) or inspections (ISO/IEC 17020).

This version of the document only presents the rights of data subjects (Art. 12 to 23) in generic terms (Section 2.12) without formulating the specific minimum requirements. The authors of this document may choose to add the specific minimum requirements to a subsequent version.

9 https://edpb.europa.eu/our-work-tools/our-documents/leitlinien/guidelines-12018-certification-and-identifying-certification_de

2.2 Art. 5: principles related to the processing of personal data

Legal criteria	*Aspects to be covered by the certification criteria and implementation by the customers[10] of the certification body[11]*	*How will the certification body verify implementation?*
Point (a) of Art. 5 (1) Lawfulness, fairness and trans-parency	Lawfulness, cf. Chapter 2.3 (Art. 6)	Cf. Section 2.3 (Art. 6)
	Fairness	Cf. Section 2.3 (Art. 6)
	Transparency of processing for data subjects: Art. 12 *et seq.* - there must be criteria for assessing whether per-sonal data is processed in a transparent manner in relation to data subjects; and - in particular, information must be provided about risks, rules, safeguards and rights, and how these	The certification body will examine documented data flows, records of processing activities, information pro-vided under Art. 13 and 14, and the documentation of the process to ensure and maintain transparency in re-lation to data subjects. The certification body will inspect all relevant business processes and systems; it will also conduct plausibility

10 This not only means the actual customers of the certification body, but also any contractual partners of the customers (e.g. processors).
11 This column essentially contains two pieces of information: a list of aspects to be covered by the certification criteria to verify compliance with the most important legal requirements, as well as measures to be taken by customers to implement those legal requirements.

	rights can be exercised (Recital 39). The processes used to select and implement technical and organisational measures must be documented in a way that ensures the transparency of processing (key objective: transparency).	analysis for all data flows. The certification scheme must at least require the certification body to check the technical and organisational measures to ensure that the requirements for ensuring transparency are met. (Document check, methodological analysis).
Point (b) of Art. 5 (1) Purpose limitation	Purpose limitation, cf. Chapter 2.3 (Art. 6) The process used to select and implement technical and organisational measures must be documented in a way that ensures that processing is limited to a specific purpose (key objective: no interlinking).	Cf. Section 2.3 (Art. 6) The certification scheme must at least require the certification body to check the technical and organisational measures to ensure that the requirements for ensuring purpose limitation are met. (Document check, methodological analysis).
Point (c) of Art. 5 (1) Data minimisation	As part of the certification criteria, the controller must provide evidence to prove that processing activities are being carried out in keeping with the principle of data minimisation.	The certification scheme must stipulate at least the following:

	The criteria must provide for the evaluation of this evidence to check whether the following legal requirements are met: Compliance with point (c) of Art. 5 (1): a) there must be criteria for assessing whether the processing of personal data is adequate, relevant and limited to what is necessary; and b) the processes used to ensure that personal data is always processed in a manner that is adequate and relevant to the purpose and limited to what is necessary must be documented (key objective: data minimisation).	The certification body will examine documents and conduct legal analysis for the documentation described in column 2. The certification scheme must at least require the certification body to conduct on-site inspections to check the following aspects of processing activities: specific databases and comparison with the criteria specified in column 2 a); this may be limited to a random sample. The certification scheme must require the certification body to check the technical and organisational measures to ensure that the requirements for ensuring data minimisation are met. (Document check, methodological analysis for column 2 b).
Point (d) of Art. 5 (1) Accuracy	As part of the certification criteria, the controller must provide evidence to prove that processing activities are	

	being carried out in keeping with the principle of accuracy. The criteria must provide for the evaluation of this evidence to check whether the following legal requirements are met: Compliance with point (d) of Art. 5 (1): a) there must be criteria for determining the factual accuracy of personal data; b) the processes used to determine the factual accuracy of personal data must be documented; and c) the processes used to select and implement suitable technical and organisational measures to ensure that any inaccurate data is immediately deleted or rectified must be documented (key objective: integrity in conjunction with Art. 16).	The certification scheme must stipulate at least the following: The certification body will examine documents and conduct legal analysis for the documentation described in column 2. The certification scheme must at least require the certification body to check the technical and organisational measures to ensure that the requirements for ensuring integrity are met. (Document check, methodological analysis).
Point (e) of Art. 5 (1)	As part of the certification criteria, the controller must	

Storage limitation	provide evidence to prove that processing activities are being carried out in keeping with the principle of storage limitation. The criteria must provide for the evaluation of this evidence to check whether the requirements of point (e) of Art. 5 (1) are met: a) there must be criteria for determining whether a data subject can be identified; b) there must be criteria for determining how long a data subject has to remain identifiable for the purposes of processing; c) there must be criteria for determining a suitable form in which personal data can be kept to ensure that a data subject can only be identified for as long as necessary for the purposes for which their personal data is processed; and	The certification scheme must stipulate at least the following: The certification body will examine documents and conduct legal analysis for the documentation described in column 2.
	d) there must be documentation of the process used to	d) The certification scheme must at least require the

	select and implement suitable technical and organisational measures to ensure that personal data is kept in a form that allows data subjects to be identified for no longer than necessary for the purposes for which their personal data is processed (key objective: data minimisation).	certification body to check the technical and organisational measures to ensure that the requirements for ensuring data minimisation are met (document check, methodological analysis).
Point (f) of Art. 5 (1) Integrity and confidentiality	Data processing based on the principle of integrity. Data processing based on the principle of confidentiality. In particular, the requirements specified in Art. 24, 25 (cf. Section 2.4) and 32 (cf. Section 2.7).	In particular, the requirements specified in Art. 24, 25 (cf. Section 2.4) and 32 (cf. Section 2.7).
	The processes used to select and implement technical and organisational measures in a way that ensures the integrity and confidentiality of processing must be documented (key objective: integrity and confidentiality).	The certification scheme must at least require the certification body to check the technical and organisational measures to ensure that the requirements for ensuring integrity and confidentiality are met. (Document check, methodological analysis).

Art. 5 (2) Accountability	Evidence of compliance with Art. 5 (1) (see above).	

2.3 Art. 6: lawfulness of processing

The processing of personal data is only permissible if there is a specific legal basis. Art. 6 contains the most important provisions of the GDPR in terms of the lawfulness of processing.

Legal criteria	*Aspects to be covered by the certification criteria and implementation by the customers of the certification body*	*How will the certification body verify implementation?*
Art. 6 (1) (in principle) Processing is only lawful under the conditions set out in Art. 6 (1).	a) Customers must present, examine and document a legal basis for the processing of personal data involved in each separate processing operation; processing operations with the same legal basis can be presented, examined and documented together.	The certification body will examine documents and conduct legal analysis to determine whether there actually is a legal basis; this examination and analysis will be based in particular on the following documents: privacy policy, information to be provided under Art. 13 and 14, records of processing activities pursuant to Art. 30, internal notes documenting the examination and the verification of a legal basis.
	b) If customers are "controllers", as defined in Art. 4 No. 7:	The certification body will examine documents and conduct legal analysis for the documentation described in

DSK
DATENSCHUTZKONFERENZ

	- customers must document their instructions issued to employees for checking whether there is a legal basis before carrying out the processing subject to certification or before changing / extending it; the instructions should specify how the check is to be done (e.g. in the form of guidelines), as well as information on the checking processes used by the controller; and - customers must document structures and responsibilities for checking whether there is an adequate legal basis (e.g. with involvement of the legal or data protection department or other responsible bodies if necessary).	column 2 (e.g. based on internal guidelines, work instructions or works agreements in place at the controller's company).
	c) Customers must implement and document processes and measures that lead to data being deleted once processing is no longer lawful. In particular, the requirements specified in point (e) of Art. 5 (1) must also be observed.	The certification body will examine the relevant documents and conduct at least a random inspection of the processes and measures described in column 2. It will also examine the requirements specified in point (e) of Art. 5 (1).

Point (a) of Art. 6 (1) Data subjects have given their consent for their personal data to be processed for one or more specific purposes.	a) Customers must check and document whether consent has effectively been given for - each processing operation; - each set of personal data; and - one or more specified purposes.	The certification body will examine the relevant documents and conduct legal analysis for the documentation (described in column 2 a) to examine consent (particularly whether it is complete, given voluntarily, up-to-date, consistent with the relevant purpose and comprehensible).
	b) The examination must focus on whether all the relevant requirements for consent have been met, particularly those specified in Art. 7 and 8, including: - Have arrangements been made to ensure that comprehensive and sufficiently clear declarations are obtained from data subjects (and/or their representatives) for all processing operations and purposes before the processing begins?	The certification body will inspect the processes and measures used to obtain consent. If any processing operations are already taking place, the certification body will examine random samples of the consent that has been given.
	- Is each data subject capable of giving consent and has the consent of their authorised representatives been obtained where necessary?	The certification body will examine the relevant documents, conduct legal analysis and inspect (1) the processes used to determine whether a data subject is capable of giving consent, in particular age verification, and (2) the steps taken if a data subject is deemed incapable of giving consent.

	- Has consent been given voluntarily (in particular taking into account superior / subordinate relationships and the ban on interlinking processing)? - Are data subjects able to withdraw their consent at any time and does this lead to the termination of processing (or can processing be continued on another legal basis)? - Are data subjects and, if applicable, their authorised representatives, sufficiently informed before giving their consent in keeping with the principle of transparency?	The certification body will examine the relevant documents, conduct legal analysis to examine the process by which data subjects can withdraw their consent, and conduct an inspection. This also includes examining and inspecting the processes that lead to data being deleted after data subjects have withdrawn their consent.
Point (b) of Art. 6 (1) Processing is necessary for the performance of a contract to which a data subject is party or	Customers must check and document whether the following requirements are met: a) A contract has been concluded with a data subject or	 The certification body will check the relevant documents

in order to take steps at the request of the data subject prior to entering into a contract.	steps have been taken at the request of a data subject prior to entering into a contract. In particular, any such (contractual) relationships must be distinguished from cases in which data subjects acknowledge offers in a non-binding manner (e.g. by visiting a website); they should also be distinguished from post-contractual relationships and clearly ineffective contracts.	and conduct legal analysis to determine whether a contract has been concluded with a data subject or whether steps have been taken prior to entering into a contract (in particular based on contract templates, descriptions or notes on pre-contractual relationships).
	b) All processed data is required to perform a contract or to take steps prior to entering into a contract.	The certification body will conduct legal and technical analysis to determine whether the data processing is actually necessary, as described in column 2 b) and c). It will also examine the requirements specified in point (c) of Art. 5 (1).
	c) All processing operations are required to perform a contract or to take steps prior to entering into a contract.	See b).
	d) Customers must document their structures and processes that lead to a contractual or pre-contractual relationship.	The certification body will examine the relevant documents for the structures and processes described in col-

		umn 2 d) and inspect the processes leading to a contractual or pre-contractual relationship.
	For b) to d), it is particularly important that the requirements specified in point (c) of Art. 5 (1) are also observed.	If any processing operations are already taking place, the certification body will conduct at least a random inspection of contracts or steps taken prior to entering into the contracts.
Point (c) of Art. 6 (1) Processing is necessary for compliance with a legal obligation to which the controller is subject.	Customers must check and document whether the following requirements are met: a) The controller is subject to a legal obligation; if so, the controller must describe the conditions under which the obligation arises, the scope of the obligation and the circumstances that may cause the obligation to expire. If the wording is not clear, it may be useful to provide documents to aid interpretation (e.g. commentaries, legal opinions, case law). b) All processed data is required to comply with the legal obligation in question.	The certification body will analyse the documentation described in column 2 a) to determine whether the controller is actually subject to a legal obligation. The certification body will conduct legal and technical

		analysis to determine whether the data processing is actually necessary for the controller to comply with a legal obligation, as described in column 2 b) and c).
	c) All processing operations are required to comply with the legal obligation in question. For b) to c), it is particularly important that the requirements specified in point (c) of Art. 5 (1) are also observed.	See b). It will also examine the requirements specified in point (c) of Art. 5 (1).
	d) The provisions referred to in Art. 6 (2) and (3) and any other special provisions must be observed.	The certification body will examine the relevant documents and conduct legal analysis to verify compliance with the regulations described in column 2 d).
Point (d) of Art. 6 (1) Processing is necessary to protect the vital interests of a data subject or another natural person.	Customers must check and document whether the following requirements are met: a) The vital interests of a data subject or another natural person are at stake. In particular, the controller is expected to detail whose and which vital interests are concerned.	 The certification body will conduct legal analysis for the documentation described in column 2 to determine whether the vital interests of a natural person are at stake.

	b) All processed data is required to protect vital interests.	The certification body will conduct legal and technical analysis to determine whether the data processing is actually necessary to protect vital interests, as described in column 2 b) and c). It will also examine the requirements specified in point (c) of Art. 5 (1).
	c) All processing operations are required to protect vital interests.	See b).
	For b) to c), it is particularly important that the requirements specified in point (c) of Art. 5 (1) are also observed.	
Point (e) of Art. 6 (1) Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.	Customers must check and document whether the following requirements are met:	
	a) The controller has been instructed to perform a task in the public interest or in the exercise of official authority. The controller is expected to describe the conditions under which the task is to be performed,	The certification body will conduct legal analysis for the documentation described in column 2 to determine whether the controller has been assigned a task pursuant to point (e) of Art. 6 (1).

	the scope of the task, and the circumstances that may cause these requirements to expire.	
	b) All processed data is required to perform the task in question.	The certification body will conduct legal and technical analysis to determine whether the data processing is actually necessary for the performance of the task in question, as described in column 2 b) and c). It will also examine the requirements specified in point (c) of Art. 5 (1).
	c) All processing operations are required to perform the task in question. For b) to c), it is particularly important that the requirements specified in point (c) of Art. 5 (1) are also observed.	See b).
	d) In particular, the provisions referred to in Art. 6 (2) and (3) and any other special provisions (e.g. depending on the scope of application) must be observed.	The certification body will examine the relevant documents and conduct legal analysis to verify compliance with the regulations described in column 2 d).

Point (f) of Art. 6 (1) Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.	a) Customers must present, examine and document the extent to which - processing is necessary for the purposes of the legitimate interests pursued by the controller or a third party; - the processing is not carried out by public authorities in the performance of their duties; and - the controller's legitimate interests are not overridden by the interests or fundamental rights and freedoms of a data subject, in particular where the data subject is a child. b) Customers must document the process used to identify overriding interests, including specific criteria and corresponding results. In particular, the process must include a presentation of which and whose specific interests are compared and contrasted, as well as the personal data and processing operations concerned in each case.	The certification body will examine the relevant documents and conduct legal analysis for the documentation described in column 2 to determine whether the requirements specified in point (f) of Art. 6 (1) have actually been met. In particular, the certification body must check whether overriding interests have been identified and taken into account correctly in each case. Random data sets should also be examined to see whether children are or could be affected and whether this has been taken into account accordingly when identifying overriding interests. The certification body will examine and inspect the process used to identify overriding interests.

		The certification body will conduct at least a random validation of data flows between systems and services (to provide a (specified) service).
Art. 6 (4) If the purpose of processing subsequently changes and there is no legal basis for the new purpose or data subjects have not given their (effective) consent to the new purpose, special requirements apply pursuant to Art. 6 (4).	a) Customers must document the change of purpose (from which purpose to which).	The certification body will examine the documentation described in column 2 to check whether the purpose of processing has actually changed;
	b) Customers must document their justification of the change of purpose and their legal examination as to whether the change of purpose is permissible.	The certification body will examine the relevant documents and conduct legal analysis for the documentation described in column 2 to check whether the change of purpose is actually permissible;
	c) Customers must have documented measures in place to allow imminent changes of purpose to be identified and changed purposes to be checked in good time, so that further precautions can be taken where necessary (e.g. requesting further consent from data subjects).	The certification body will check documents and examine the documentation described in column 2 to verify whether measures are taken to identify changes of purpose and whether the necessary precautions are subsequently taken; it will also conduct at least a random inspection of those measures and precautions.

2.4 Art. 25: data protection by design and by default

2.4.1 Introductory remarks

The legal requirement of data protection by design (DPbD) aims to ensure that systems processing personal data are designed in such a way that they are only capable of performing processing activities that they are legally authorised to perform. The relevant legal requirements are explicitly established in Art. 25 GDPR and relate to the effective implementation of the data protection principles set out in Art. 5 GDPR, compliance with the GDPR requirements, and the rights of data subjects (particularly under the Charter of Fundamental Rights of the European Union and Chapter III GDPR). DPbD therefore involves the structured identification, analysis and assessment of all relevant normative requirements, including, where applicable, the balancing of competing legal interests and obligations.

The concept of “design” is to be interpreted broadly. It encompasses not only the design of technical systems, but also organisational design, including all phases of personal data processing and the entire lifecycle of the personal data processed within such systems.

A transparent and documented methodological approach is necessary in order to develop the technical and organisational measures (TOMs) required under Art. 25 GDPR in a reproducible manner. From a methodological perspective, two categories of requirements must be taken into account: firstly, the identified normative requirements, which must be functionally reflected in the system processing personal data; and secondly, the risks as identified in the risk assessment, which must be mitigated or eliminated by means of appropriate safeguards. This applies to certification schemes with a specific subject of certification and application context, as well as to certification schemes for generic processing activities. In the latter case, the scheme must define a methodology for developing appropriate measures rather than prescribing specific safeguards.

2.4.2 Relationship between Article 25 and Articles 32 and 35 GDPR

The second category of requirements (i.e. ensuring an appropriate level of protection for data, IT systems, IT services, interfaces, IT infrastructure components and processes) is also specifically addressed by Art. 32 GDPR. Certification criteria that merely require a (data) security concept comprising technical and organisational measures derived from a risk assessment are therefore intended to supplement criteria that address the first category of requirements.

DPbD also intersects with the requirement to conduct a data protection impact assessment (DPIA) under Art. 35 GDPR. If the threshold analysis included in the risk assessment determines that the subject of certification involves high risks, a DPIA must be conducted. Although the risk assessment required for a DPIA (lit. (c) of Art. 35 (7) GDPR) and the design of technical and organisational measures (lit. (d) of Art. 35 (7) GDPR) are already covered by DPbD, certain requirements arising from Art. 35 (e.g. those relating to the DPIA procedure and the involvement of data subjects) extend beyond the requirements of Art. 25 and must therefore be included in the certification scheme as separate criteria.

The aspects to be covered by the certification criteria, as listed in the second column of the table below, are largely based on the requirements set out in EDPB Guidelines 4/2019 on Art. 25 GDPR.

2.4.3 Tabular overview: requirements, forms of implementation and examination methods

Legal criteria	*Aspects to be covered by the certification criteria and implementation by the customers of the certification body*	*How will the certification body verify implementation?*
Art. 25 (1) Implementation of appropriate technical and organisational measures	A description of all technical and organisational measures must be available. In addition, a documented methodology must demonstrate a clear and systematic link between: • the legal requirements; • the risks associated with the processing activities (see below); and • the resulting technical and organisational measures.	The certification body will review documents, the methodological components of the relevant data protection concept and the documented measures. Examples of recognized standards or best practices include the Standard Data Protection Model (SDM)[1], the PRIPARE method, as well as the ZAWAS process.

	Recognised standards, best practices and codes of conduct should be used for this purpose. [EDPB, para. 10]	
Art. 25 (1) Implementation of appropriate technical and organisational measures • when determining the means of processing; and • during the processing itself	The identified measures must be appropriate both when determining the means of processing and during the processing itself. [EDPB, para. 33] The various aspects of data protection by design and by default must be taken into account and evaluated throughout every phase of the design of the processing activities (e.g. procurement, tendering procedures, outsourcing, development, support, maintenance, testing, storage, deletion, processing on behalf of a controller). [EDPB, para. 60] [EDPB, para. 39]	The certification body will examine the relevant project and tender documentation. The certification body will conduct interviews with employees regarding the design strategy or process model. The certification body will audit the change management process and associated documentation.
	Processing activities and the chosen measures and safeguards must be reviewed	The certification body will review the change history of the relevant data protection concept, risk assessment and risk

	and reassessed on a regular basis. [EDPB, para. 37] An effective data protection management system must be established in line with the PDCA cycle.	treatment documentation, change management documentation, data protection reports and records of processing activities. The certification body will audit the process and information sources used to track legal developments and the state of the art, and will also review training records.
Art. 25 (1) Effective implementation	The implemented measures and safeguards must deliver the intended data protection outcomes (effectiveness). Appropriate KPIs[2], both quantitative and qualitative, must be defined and continuously monitored to demonstrate effectiveness. [EDPB, para. 16] The monitoring of these KPIs should, to the greatest extent possible, be supported by IT-based monitoring systems.	The certification body will conduct an on-site inspection and audit, in particular to verify the effectiveness of monitoring and event management systems, notification systems, definition and logging of KPIs, CI/unit testing practices, test frameworks, unit and integration testing in CI/CD[3] pipelines and test coverage metrics.

		The certification body will review functional test reports, penetration test documentation, project reports and audit reports.
Art. 25 (1) Consideration of the state of the art	When determining appropriate technical and organisational measures, the “state of the art” (i.e. the current level of technological development on the market) must be taken into account. [EDPB, para. 19] A process must be in place for the regular identification and evaluation of the state of the art and for the corresponding adaptation of processing activities. [EDPB, para. 20] The “state of the art” requirement applies not only to technical measures, but also to organisational measures. [EDPB, para. 21]	The certification body will review project or decision-making documentation with regard to the various organisational or technical solutions, including the factors considered in balancing different options (e.g. type of data, risks, costs). The certification body will interview employees to find out which measures are taken to monitor the state of the art and whether suggestions for updating the means of processing are appropriately taken into account. The certification body will review training records relating to the latest developments

		in technology, security and data protection. The certification body will review records demonstrating the sources consulted (e.g. standards, sectoral and industry standards, guidance papers and implementation guidance issued by supervisory authorities). [EDPB, para. 22]
Art. 25 (1) Consideration of the cost of implementation	Where implementation costs are considered as a relevant factor, the controller must be able to manage the overall costs in a way that allows for the adoption of alternative measures that require fewer resources while still effectively ensuring compliance with the principles. Even where measures do not conform to established standards, they must still be appropriate and effective. [EDPB, para. 25] When determining appropriate measures for data protection by design, the controller may	The certification body will review documentation relating to alternative appropriate measures and their effectiveness in cases where such measures are not covered by standards reflecting the state of the art.

	not use implementation costs as a justification for failing to implement data protection by design.	
Art. 25 (1) Consideration of the nature, scope, context and purposes of processing	The nature, scope, context and purposes of the processing activities must be correctly identified. The nature, scope, context and purposes of the processing activities must be considered when defining the necessary measures. [EDPB, para. 26] Special categories of personal data (e.g. categories of data covered by Art. 9 GDPR and personal data relating to children) must be appropriately taken into account. [EDPB, para. 28]	The certification body will review the relevant records of processing activities, the data protection concept, the organisational chart and data flow diagrams showing interfaces.
Art. 25 (1)	A risk assessment must be conducted. [EDPB, para. 30]	The certification body will review the documented risk assessment processes and the provisions in data protection and security policies specifying the standards to

Consideration of the varying likelihood and severity of the risks posed by the processing to the rights and freedoms of natural persons	The risk assessment must focus on natural persons and the risks to their rights, while taking into account the characteristics of the processing activities (nature, scope, context and purpose). 29]	be used for risk assessment (e.g. DIN ISO 31000, SDM, BSI Standard 200-3[4]).
	A risk assessment methodology must be defined and applied that includes the following elements: threat model (sources of risk), risk identification, risk analysis and risk evaluation. [EDPB, paras. 85, 31, in conjunction with WP 248, p. 21] [DIN ISO 31000, p. 19]	The certification body will review documents and the methodological components of the relevant information security concept and data protection concept, as well as risk assessment[5] and treatment documentation. The certification body will conduct an on-site inspection and audit to verify the effectiveness of vulnerability scanners, SIEM systems[6] and SCA systems[7].
	The likelihood and severity of the risks must be assessed as part of the risk analysis. [EDPB, para. 30]	The certification body will review documents and methodological aspects relating to the assessment and treatment of risks.

	Even if baseline scenarios, best practices and standards are used, a case-by-case assessment of the data protection risks posed by the processing activities must always be conducted under Art. 25 (and Art. 24, 32 and 35), together with an assessment of the effectiveness of the measures and safeguards. [EDPB, para. 32]	See preceding rows.
Art. 25 (2) The appropriate technical and organisational measures must ensure that data minimisation is achieved by default in relation to: • the amount and extent of processing; • the storage period; and • accessibility.	Default processing settings and options must be chosen in such a way that only processing that is strictly necessary to achieve the specified lawful purpose is carried out by default. [EDPB, para. 42]	The certification body will review documents and analyse processing activities and the relevant purposes from a legal perspective, based on the records of processing activities, the data protection concept and the IT concept. The certification body will conduct an audit, in particular a technical inspection of configuration files and default settings in the user interface.

	If the controller uses any third party-applications or off-the-shelf software, the controller must conduct a product risk assessment and make sure that functions that do not have a legal basis or are not compatible with the intended purposes of processing are switched off. [EDPB, para. 44]	The certification body will review the relevant risk assessment / treatment documentation or DPIA.
	Any personal data that has been collected must not be stored if it is not necessary for the purpose of the processing and if there is no other compatible purpose or legal basis. [EDPB, para. 52]	The certification body will audit the relevant interfaces and transfer points, in particular in cases where personal data has not been obtained directly from the data subject.
	If data anonymisation is required and/or appropriate, a systematic anonymisation procedure must be integrated into the processing activities. Where available, this should be carried out in accordance with EDPB guidelines. [EDPB, para. 53]	The certification body will review the relevant anonymisation concept, independently prepared security analysis and, where applicable, DPIA (e.g. if anonymisation is incomplete).

Specifically with regard to data minimisation in terms of the amount and extent of processing	When defining categories of personal data, the controller must justify why not processing them would prevent the intended purpose from being achieved. With regard to the volume of personal data collected (e.g. in the case of sensor data sets), the controller must justify why excluding a subset of that data would prevent the intended purpose from being achieved. [EDPB, para. 76] Both aspects must be taken into account in particular when using third-party applications or commercial off-the-shelf software. [EDPB, para. 76] If possible, aggregated data should be processed instead of data that allows direct identification of individuals. [EDPB, para. 76]	The certification body will review documents and conduct legal analysis based on the data protection concept.
	Where necessary and/or appropriate, personal data must be pseudonymised as soon	The certification body will conduct an audit, in particular a technical inspection of

	as directly identifiable personal data is no longer required. The identification key must be stored separately and securely. [EDPB, para. 76] Where data transmission can be implemented in different ways, preference should be given to approaches that avoid creating more copies than necessary[8]. [EDPB, para. 76]	the relevant data protection concept, pseudonymisation concept, independently prepared security analysis, documentation of pseudonymisation transformation rules and functional test reports.

Specifically with regard to data minimisation in terms of storage periods	The retention period must be limited to what is necessary for the purpose, and a systematic deletion procedure must be in place. [EDPB, para. 53]	The certification body will review the relevant data protection concept, deletion concept and deletion logs. The certification body will conduct an audit, in particular a technical inspection of scheduled tasks and functional test reports.
Specifically with regard to data minimisation in terms of accessibility, in particular ensuring that, by default, personal data is not made accessible to an indefinite number of natural persons without the data subject's intervention.	The group of persons who have access to personal data, and the type of access granted in each case, must be determined on the basis of a needs assessment.	The certification body will review the relevant data protection concept, role and access rights concept, directory service and identity management system.
	The controller must ensure that, when needed, personal data is actually accessible to those who require it (e.g. in critical situations). [EDPB, para. 55]	The certification body will review the relevant emergency response plan and functional test reports.

	The controller must ensure that personal data is not made accessible to an indefinite number of natural persons without the data subject's intervention (e.g. by making it searchable through search engines). [EDPB, para. 56]	The certification body will conduct an audit, in particular a technical inspection of default settings in the user interface, firewall systems, search engine information (e.g. robots.txt), publicly accessible interfaces and functional test reports.
Data protection principles / data protection safeguarding objectives		
Implementation of the principle of transparency	Appropriate measures must be taken to ensure that data subjects are informed clearly and transparently about how personal data is to be collected, used and disclosed. [EDPB, para. 65]	The certification body will audit the information provided and its accessibility, cross-checking such information against the relevant data protection concept and records of processing activities.

	Information must be provided in an easily accessible, multi-layered format across multiple communication channels, using language that can be understood by both humans and machines. [EDPB, para. 66]	
	Organisational measures must be in place to ensure that the information is kept up to date at all times.	The certification body will examine the relevant documents, conduct interviews and review the change management process to ensure that information for data subjects is kept up to date.
Implementation of the principle of lawfulness	Appropriate measures must be taken to ensure that all processing activities are lawful. [EDPB, para. 67] The measures and safeguards must support compliance with the applicable legal requirements and ensure that the entire processing lifecycle remains consistent with the relevant legal basis. [EDPB, para. 67]	The certification body will review documents and conduct legal analysis in relation to the relevant data protection concept, privacy policy for data subjects and input forms containing the relevant checkboxes for obtaining and withdrawing consent.

	Where processing is based on consent, such consent must be obtained separately for each purpose. [EDPB, para. 68] It must be just as easy for data subjects to withdraw consent as it is to give it. [EDPB, para. 68]	
	If there are any changes to the relevant legal basis, the processing activities must be reviewed and adapted accordingly. [EDPB, para. 68]	The certification body will audit the relevant change management documents.
	The controller's applications must be designed in such a way that processing will be stopped immediately if the legal basis ceases to apply (e.g. upon withdrawal of consent). [EDPB, para. 68].	The certification body will conduct an audit, in particular a technical inspection of the relevant consent management system and functional test reports.
	Where processing is based on legitimate interests, the controller must conduct a balanced assessment of the competing interests, taking particular account of any power	The certification body will review the documented balancing of interests.

	imbalance, especially where children or other vulnerable groups are involved. Measures and safeguards must be implemented to mitigate any adverse effects on data subjects. [EDPB, para. 68] [Please refer to section on lit. (f) of Art. 6 (1) in the assessment criteria paper]	
Implementation of the principle of fairness	Appropriate measures must be taken to safeguard the fundamental rights and freedoms of data subjects. [EDPB, para. 69] [EDPB, para. 70] The system must be designed in such a way that the fundamental rights and freedoms of data subjects are effectively protected against the following threats in particular: • unexpected processing; • discrimination; • exploitation of vulnerability;	The certification body will review the relevant data protection concept and risk assessment.

	• lock-in effects (effectively undermining the right to data portability); • exploitation of power imbalances; • transfer of risks to data subjects; and • manipulation, fraud and deception.	
	The system must be designed to support user interaction, enabling data subjects to exercise their rights, and to ensure human intervention, without any automated decision-making. [EDPB, para. 70]	The certification body will conduct an audit, in particular a technical inspection of mechanisms enabling differentiated consent, withdrawal of consent and objection, data fields for blocking indicators, notifications, consent records, objections and statements of opposition, options to disable individual functions without affecting the overall system, query and dialogue interfaces for data subjects, a single point of contact, and operational capabilities to ensure the consistent correction, restriction and deletion of all personal data stored for a data subject.

	All programme workflows must be regularly reviewed to check whether they are functioning as intended for their specified purpose. [EDPB, para. 70]	The certification body will review the relevant audit records.
Implementation of the principle of integrity and confidentiality	The controller must continuously assess whether appropriate means are being used for processing and whether the chosen measures are effectively addressing any vulnerabilities. [EDPB, para. 84]	The certification body will conduct an audit, in particular a technical inspection of the relevant test concept, logging, vulnerability scanners and SIEM system.
	Operational resources must be available to support the management of information security strategies and procedures. [EDPB, para. 85]	The certification body will audit the relevant information security management system.
	Security requirements must be integrated into all stages of system design and development. [EDPB, para. 85]	The certification body will review the relevant information security concept, data protection concept, requirements management system, project documentation and change management documentation.

	Tests for security requirements must be developed, integrated into the process and executed on an ongoing basis. [EDPB, para. 85]	The certification body will conduct an audit, in particular a technical inspection of the relevant test concept, test frameworks, automated unit tests in CI/CD pipelines and test coverage metrics.
	Applications, devices, systems, services and similar components must be regularly reviewed and tested to identify any vulnerabilities in the systems intended to support processing. [EDPB, para. 85]	The certification body will conduct an audit, in particular a technical inspection of the relevant test concept, monitoring and event management system, inspection round logs, failover test reports and recovery test reports.

	Access control management must ensure that access to personal data is restricted to authorised employees who require it to perform their processing tasks, with the number of authorised persons kept to a minimum. [EDPB, para. 85]	The certification body will conduct an audit, in particular a technical inspection of the relevant role and access rights concept, directory service and IAM system.
	For individual processing activities, access should be restricted to specific data fields within each record that are required to perform the task in question. [EDPB, para. 85]	The certification body will conduct an audit, in particular a technical inspection of the relevant role and access rights concept, input masks and search masks.
	In the design of task-segregated data processing, it must be ensured that no single individual has comprehensive access to all data collected on a data subject, let alone to all personal data relating to a specific category of data subjects. [EDPB, para. 85]	The certification body will conduct an audit, in particular a technical inspection of the relevant role and access rights concept, administration concept, directory service and IAM system.
	The transmission of personal data must be protected against unauthorised or accidental access and alteration. [EDPB, para. 85]	The certification body will review the relevant information security concept and cryptographic concept.

		The certification body will conduct an audit, in particular a technical inspection of key management, configuration files and functional test reports (including analysis of captured network traffic).
	Data storage systems must be designed in such a way that they are protected against unauthorised access and alteration. [EDPB, para. 85]	The certification body will review the relevant role and access rights concept, administration concept, IT concept and penetration test documentation. The certification body will conduct an audit, in particular a technical inspection of data storage systems.
	The controller must assess whether the pseudonymisation of personal data (e.g. via encryption) is necessary and/or appropriate to minimise the risks of unauthorised disclosure and must implement such measures accordingly. [EDPB, para. 85]	The certification body will review the relevant data protection concept, pseudonymisation concept, mapping tables, documentation of pseudonymisation transformation rules, functional test reports and independently prepared security analysis.

	The controller must ensure that all systems storing personal data (e.g. back-ups, log files, test systems and data warehouses) are protected against unauthorised or accidental access and alteration, and that such systems are subject to regular monitoring. [EDPB, para. 85]	The certification body will review the relevant role and access rights concept, back-up and recovery concept, logging concept, administration concept and functional test records (including access and authentication tests). The certification body will conduct an audit, in particular a technical inspection of system access mechanisms.
	Disaster recovery and business continuity requirements for the information system must be taken into account to ensure that the availability of personal data can be restored after major incidents. [EDPB, para. 85]	The certification body will review the relevant emergency response plan and recovery test reports.
	If possible, any personal data that involves special risks must be stored separately. [EDPB, para. 85]	The certification body will review the relevant data protection concept, risk assessment, security zoning concept and segregated file systems, database systems, virtualisation infrastructures, hardware, networks and data centres.

	Processes, procedures and resources must be deployed to detect, contain, manage and report personal data breaches and to draw lessons from such breaches. [EDPB, para. 85]	The certification body will audit the relevant data protection concept, whistle-blower reporting channel, bug bounty programme, monitoring and event management system, SIEM system, incident management process, logs of personal data breaches and training records.
Implementation of the principle of purpose limitation	Processing must be designed, and its boundaries defined, in line with the specified purposes. [EDPB, para. 72] [Please refer to section on lit. (b) of Art. 5 (1)]	The certification body will review the design and documentation of processing activities, in particular the relevant records of processing activities, privacy policy, data protection concept and data processing agreements.
	Data storage and processing must be separated in such a way that further processing for new purposes incompatible with the original purpose is only possible with disproportionate effort. [EDPB, para. 72]	The certification body will conduct an audit, in particular a technical inspection of the segregated file systems, database systems, virtualisation infrastructures, hardware, networks and data centres, as well as multi-tenant systems based on the data

		protection concept, IT concept and information security concept.
	Both technical measures (e.g. hashing, encryption) and organisational measures (e.g. strategies, contractual obligations) must be implemented to minimise the risk of personal data being used for new purposes. [EDPB, para. 72]	The certification body will review the relevant data protection concept, role and access rights concept, cryptographic concept, functional test reports and contracts.
Implementation of the principle of accuracy	Where appropriate, the source of personal data should be reliable with regard to data accuracy, and data subjects should be able to interact with the system to rectify their data if necessary. [EDPB, para. 79]	The certification body will audit the processes implemented by the controller and conduct a technical inspection of input masks after log-in / authentication, as well as functional test reports (including notifications following rectification).
	If possible, the correct results for given inputs must be determined. Any deviations must then be regularly assessed through sampling or during the testing phase to es-	The certification body will conduct an audit, in particular a technical inspection comparing deviations in test results and samples before and after improvement.

	tablish measurable accuracy. These deviations must be reduced to ensure lower error rates for future inputs.	
	Depending on the type of data and how frequently it may change (e.g. age-related requirements), the controller must ask data subjects to verify the accuracy of their personal data before processing and at various stages during processing. [EDPB, para. 79]	The certification body will audit the relevant data protection concept, IT concept and documentation of verification requests.
	Incorrect data must be promptly rectified or erased across the entire processing chain. The controller must ensure this in particular where data subjects are or were children and subsequently request the deletion of their personal data. [EDPB, para. 79]	The certification body will conduct an audit, in particular a technical inspection of the relevant deletion concept and functional test reports.
	Personal data must remain accurate throughout all stages of processing; in critical phases, its accuracy should be verified using appropriate qualified methods. [EDPB, para. 79]	The certification body will audit risk assessment and treatment, documentation of verification processes and/or services and documentation of verification requests.

	Technical and organisational design features must be implemented to reduce inaccuracy (e.g. concise, pre-defined response options should be used instead of free text fields). [EDPB, para. 79]	The certification body will conduct an audit, in particular a technical inspection of the relevant data protection concept and input masks.

2.5 Art. 26:

2.5.1 Introductory remarks

The starting point for determining whether there are joint controllers is the subject of certification described in Section 2.1.1 above. If the processing activities described there are likely to have joint controllers based on the criteria below, the application for certification (ISO 17065, 7.2) must be filed by all joint controllers. All joint controllers must have a legally enforceable agreement with the conformity assessment body.

2.5.2 Tabular overview: requirements, forms of implementation and examination methods

Legal criteria	*Aspects to be covered by the certification criteria and*	*How will the certification body verify implementation?*

	implementation by the customers of the certification body	
First sentence of Art. 26 (1) Joint determination of the purposes and means of processing	With regard to controllership, see requirement in point 6 of Section 2.1.2 above. Here are the criteria for a two-step check based on the EDPB Guidelines 07/2020[12]: **Step 1: Those concerned have verified their status as "controllers", as defined in Art. 4 No. 7**, in relation to all or individual processing steps. The following criteria must be examined in relation to the specific subject of certification: a) legal[13] or actual (co-)determination of purposes (why data is processed)[14]; and	The certification body will conduct legal analysis to check whether any legal regulations apply to the tasks performed by each controller. The certification body will examine the documentation of decision-making processes regarding the purposes and (essential) means of processing. The certification body will check the relevant contract and other documents from those involved (e.g. privacy

12 Guidelines 07/2020 on the concepts of controller and processor in the GDPR, Version 2.0.

13 If a (joint) controller is nominated by law, this may either result from the provisions of Art. 4 No. 7 or implicitly from the legal assignment of a task to a controller in accordance with the EDPB Guidelines 07/2020, para. 24.

14 Usage data / metadata must also be taken into account.

		policy), as well as the records of processing operations.
	b) legal or actual (co-)determination of the means of processing (how data is processed), distinction between essential and non-essential means (cf. EDPB Guidelines 07/2020, para. 39 f.) for the subject of certification, in particular the power to decide “which data” and “how long”.	The certification body will conduct an audit, including random technical checks to determine the extent to which the main findings of the document check correspond to the actual processing.
	Step 2: The means and purposes of processing are jointly determined in relation to all or individual processing steps. (Distinction from cases in which there are two or more independent controllers). Joint participation can also take the form of “converging decisions” (cf. EDPB Guidelines 07/2020, para. 54 f.). Joint participation refers to a controller’s authority to determine	

	a) the purposes; and b) the (essential) means of processing[15].	
Second and third sentence of Art. 26 (1) ; first and second sentence of Art. 26 (2)	Customers must examine and document the extent to which the tasks to be performed by each controller are governed by law. If the tasks to be performed by each controller are not governed by law, they must establish a transparent contractual arrangement according to the second sentence of Art. 26 (1). The following points are particularly important: - full coverage of obligations under the second sentence of Art. 26 (1); - measures to comply with data protection principles and honour the rights of data subjects, and a definition of each party's obligations; and - clarity, comprehensibility and transparency of the	The certification body will examine the documentation based on the relevant legal situation and practice. The certification body will examine the arrangement to be made between the joint controllers. It will also examine records of their processing activities. Furthermore, the certification body will examine process descriptions, verify the implementation and effectiveness of those processes (particularly for the exercise of data subjects' rights) and audit the processes (e.g. by simulating input from data subjects). The certification body will examine process descriptions

15 For more information, please refer to the EDPB Guidelines 07/2020, para. 53.

	agreement (in particular with regard to the delimitation of roles and responsibilities). - If the joint controllers make use of the option of designating a point of contact for data subjects in accordance with the third sentence of Art. 26 (1), there must be a specific process description for the functions to be assumed by the point of contact, and the contractual arrangements must duly reflect the respective roles and relationships of the joint controllers vis-à-vis data subjects, cf. first sentence of Art. 26 (2).	relating to the second sentence of Art. 26 (1) and, if applicable, the third sentence of Art. 26 (1) (point of contact). It will also verify the implementation and effectiveness of those processes (e.g. by simulating internal and external incidents). The certification body will conduct an audit to examine the arrangements for the implementation of technical and organisational measures with regard to the dependencies, overlaps and roles of the joint controllers, including their obligations to provide (mutual) support. The certification body will examine the arrangements for cross-departmental risk analysis[16], threshold value checks pursuant to Art. 35 (1) and, if relevant, the fulfilment of obligations under Art. 35 and 36.

16 Technical and organisational measures always imply a risk analysis (Art. 24: “severity of risks”). In the case of Art. 26, risk analysis should be carried out jointly by the controllers; if the risk analysis is carried out separately, certain risks might not be identified by any of the joint controllers or each controller might think that the other parties are responsible for risks in that particular area.

	The joint controllers must make[17] the essence of their contractual arrangement[18] available to data subjects in accordance with the second sentence of Art. 26 (2).	The certification body will examine the arrangements for the inclusion of additional contractual partners and the use of processors, where applicable. The certification body will examine the information provided to data subjects (in particular with regard to its clarity, comprehensibility, accessibility and the transparency of role definitions).
Art. 26 (3)	The following examination criteria must be met: - each controller must have roles and processes in place to enable data subjects to exercise their rights; - there must be arrangements and processes in place to prepare for the eventuality that a certain controller is unable to honour the rights of a data subject alone; - there must be processes in place to prepare for the eventuality that the other controller fails to honour	The certification body will examine the relevant contractual arrangements. The certification body will examine the relevant process descriptions and conduct an audit for those processes (e.g. by simulating input from data subjects).

17 Cf. EDPB Guidelines 07/2020, para. 181.
18 Cf. EDPB Guidelines 07/2020, para. 180.

	the data subject's right despite being able to; and - there must be processes in place to prepare for the eventuality that data subjects exercise their rights against more than one controller, as specified in Art. 26 (3), and data subjects must be made aware of this option.	The certification body will examine the information provided to data subjects.

2.6 Art. 28: processors

2.6.1 Introductory remarks

When applying the assessment criteria under this section, two scenarios must be distinguished:

- A controller's processing activities are to be certified. If the controller engages processors in this context, the processing activities carried out by such processors are also included in the processing subject to certification.
- A processor's services are to be certified.

Art. 28 is the key provision governing processors under the GDPR. Art. 28 (1) stipulates that controllers may only engage processors that provide sufficient guarantees to implement appropriate technical and organisational measures in such a way that processing complies with the GDPR and safeguards the rights of data subjects.

If a controller's processing activities are to be certified, the assessment also covers the contractual and other legal obligations of all (sub-) processors involved to provide adequate guarantees for GDPR-compliant processing. Only demonstrable guarantees may be taken into account when assessing compliance with the controller's obligations[1]. Such guarantees may include approved codes of conduct under Art. 40 GDPR or certifications under Art. 42 GDPR. The obligation to engage only processors that provide appropriate guarantees is ongoing; controllers should therefore verify such guarantees at reasonable intervals, including through **audits or inspections**[2] where appropriate.

The involvement of processors (or sub-processors) must not reduce the level of protection for the rights of data subjects compared to direct processing by the controller[3]. In particular, this means that processors must use technologies that allow the controller to apply the **settings required** under Art. 24 and 25 GDPR and to monitor processing using **appropriate technical means.**

If a processor's services are to be certified, the processor must therefore demonstrate that they (and any sub-processors) have implemented the necessary technical and organisational measures within their sphere of control or have enabled the controller to implement such measures (e.g. via configuration options).

2.6.2 Tabular overview: requirements, forms of implementation and examination methods

Legal criteria	*Aspects to be covered by the certification criteria and implementation by the customers of the certification body*	*How will the certification body verify implementation?*
Preliminary review: In which capacity under data protection law is the **applicant** requesting certification – as a	Two scenarios must be distinguished: 1. A controller's processing activities are to be certified. If the controller engages processors in this context, the processing activities	

controller or as a processor?	carried out by such processors are also included in the processing subject to certification. • The certification applies to the controller and does not extend to any processors engaged by the controller. 2. A processor's services are to be certified. • The certification applies to the processor and does not extend to any sub-processors engaged by the processor. <u>Assessment note</u>: In the first scenario, Art. 28 (1) GDPR must be assessed directly in the relationship between controller and processor. In the second scenario, Art. 28 (1) GDPR must be assessed indirectly in conjunction with Art. 28 (4)	

	GDPR, as the processor subject to certification has already been selected and engaged by a controller. As the obligations of sub-processors must "mirror" those of processors under Art. 28 (4) GDPR, many assessment steps are similar in both cases. In the second scenario, it should be noted that the processor subject to certification not only processes personal data as a processor on behalf of the controller, but also acts as an independent controller for certain pro-cessing activities (e.g. processing of the controller's personal data as a contractual counterparty under lit. (b) of Art. 6 (1) GDPR).	
Art. 4 No. 8 Is data being processed by a **processor**?	A processor (Art. 4 No. 8 GDPR) processes personal data on behalf of a controller (Art. 4 No. 7 GDPR). The controller determines the <u>purposes</u> ("why?") and the <u>essential means</u> ("how?") of the processing. The processor may only exercise discretion with respect to <u>non-essential means</u>. Sub-processors are also processors within the meaning of Art. 4 No. 8 GDPR. Regardless of the number of (sub-)processors involved in the processing, the controller remains responsible and accountable for the entire pro-cessing chain up to the final processing step.	Please refer to section on Art. 26

	• Is processing by a processor legally permissible? (e.g. not applicable under Section 11 of the German Tax Advisory Act [StBerG]) • Distinction from processing by an independent controller (cf. EDPB Guidelines 07/2020 on the concepts of "controller" and "processor" under the GDPR (Version 2.0, adopted on 7 July 2021), hereinafter referred to as "Guidelines 07/2020", paras. 82, 83 • Distinction from joint controllership within the meaning of Art. 26 GDPR (cf. Guidelines 07/2020, para. 46 ff.)	
Art. 28 (1) **Selection** of processor	The controller may only engage processors that provide sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of the GDPR and will ensure the protection of the rights of data subjects (Art. 28 (1) GDPR), (cf. Guidelines 07/2020, paras. 94-99 ff.).	Where available, the certification body will review evidence of compliance with approved codes of conduct under Art. 40 GDPR or data protection certification under Art. 42 GDPR (cf. Art. 28 (5) GDPR), provided they are compatible with the nature, circumstances, scope, and

	For this purpose, the controller must assess whether the processor meets the requirements of Art. 28 (1) GDPR, particularly in terms of expert knowledge, reliability and resources (Recital 81 GDPR)[4]. The controller must document its decision regarding the selection of the processor, including the evidence submitted for this purpose.	purposes of the controller's processing. Alternatively or additionally, the certification body will review the list of processors engaged by the controller. The certification body will review contracts (e.g. liability clauses and contractual penalties), use cases, exclusion criteria and security classification models. The certification body will review documents submitted by the processor, such as its privacy policy, terms of service, records of processing activities, document management policies, information secu-

		rity concept, external data protection audit reports and recognised international certifications such as the ISO/IEC 27000 series (cf. Guidelines 07/2020, para. 95) The certification body will review functional test reports prepared before or during the pilot deployment of the service.
	Similarly, a processor may only engage sub-processors that also meet the requirements of Art. 28 (1) GDPR (Art. 28 (4) GDPR).	The certification body will review the list of sub-processors engaged by the processor.
	The configuration options offered by the processor must enable the controller to fulfil its obligations under Art. 5 (2), 24 and 25 GDPR[5].	The certification body will conduct an audit, in particular a technical

	These configuration options must be sufficiently comprehensive to ensure that the controller can implement the measures required under Art. 25 GDPR at all times, either by configuring them directly or by instructing the processor accordingly.	inspection of the relevant data protection concept and configuration options, including the rationale for restrictions and additional safeguards, as well as the process for handling instructions from the controller.
Art. 28 (2) and (4) Sub-processors	• Selection of suitable sub-processors: The same requirements apply as for selecting processors under Art. 28 (1) GDPR *(please refer to the explanations above relating to Art. 28 (1) GDPR)*. • The processor must obtain prior specific or general written authorisation before engaging each sub-processor. • The processor must ensure that the same data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Art. 28 (1) and (3) are also imposed on the sub-processor by way of a contract or other legal act.	For sufficient guarantees, *please refer to the explanations above relating to Art. 28 (1) GDPR*. The certification body will conduct an audit, in particular a technical inspection of the notification system and feedback channel for approvals / objections with defined deadlines.

Art. 28 (3) **Contract** or **other legal act** as the basis for engaging a processor	Processing by a processor must be governed by a <u>contract</u> or <u>other legal act</u> under Union or Member State law that is binding on the processor in relation to the controller. **Please note**: In contrast to a contract, "<u>other legal acts</u>" are likely to have little practical relevance in certification procedures. Such "other legal acts" are more likely to arise in the context of hierarchical relationships between public authorities (e.g. in the form of an administrative decree). Nevertheless, the term "other legal instrument" is included below for the sake of completeness.	The certification body will review the relevant documents.
Art. 28 (3) **Minimum content** of the contract or other legal act	<u>First sentence of Art. 28 (3) GDPR</u>: <u>To be clearly and comprehensively specified</u>: • subject matter of processing; • duration of processing; • nature of processing; • purpose of processing; • types of personal data; • categories of data subjects; and	The certification body will review the data processing agreement, documented changes to sub-processor arrangements and documented instructions from the controller.

	• rights and obligations of the controller (insofar as not already covered by Art. 28 (1) and Art. 28 (3) GDPR). lit. (a) to (h) of Art. 28 (3) GDPR: • The processor may only process personal data on documented instructions from the controller, including in relation to transfers to third countries (lit. (a) of Art. 28 (3) GDPR). • The processor must ensure that persons authorised to process personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality (lit. (b) of Art. 28 (3) GDPR).	

	• The processor must implement all measures required under Art. 32 GDPR (lit. (c) of Art. 28 (3) GDPR). • The processor must comply with the conditions set out in Art. 28 (2) and (4) GDPR for engaging another processor (lit. (d) of Art. 28 (3) GDPR); in particular, prior written authorisation must be ensured (EDPB Guidelines 07/2020, paras. 151 ff.), and sub-processors must be precisely identified along with their specific tasks. • The processor must assist the controller in fulfilling its obligation to respond to data subject requests (lit. (e) of Art. 28 (3) GDPR). • The processor must assist the controller in ensuring compliance with Art. 32 to 36 GDPR (lit. (f) of Art. 28 (3) GDPR).	

	• Once the processing services have been fully provided, the processor must delete or return all personal data at the controller's discretion (lit. (g) of Art. 28 (3) GDPR). • The processor must provide the controller with all information necessary to demonstrate compliance with the obligations laid down in Art. 28 GDPR and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller (lit. (h) of Art. 28 (3) GDPR) → please also refer to the following section on "Demonstration of compliance". <u>Art. 28 (3) GDPR</u>: The processor must inform the controller without undue delay if it believes that an instruction infringes data protection law.	
lit. (h) of Art. 28 (3)	In accordance with lit. (h) of Art. 28 (3) GDPR, the processor must provide the controller with all information necessary to demonstrate compliance	The certification body will conduct an audit, in particular a technical

Demonstration of compliance	with the obligations laid down in Art. 28 GDPR and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller. The processor must provide an appropriate monitoring system to continuously and retrospectively verify legal compliance and demonstrate the effectiveness of implemented measures (lit.s (c) and (h) of Art. 28 (3) in conjunction with Art. 5 (2), lit. (d) of Art. 32 (1), Art. 24 and Art. 25 (1) GDPR).	inspection of the relevant monitoring concept and system, key performance indicators and thresholds, as well as the notification system for threshold breaches or substantial functional changes.
Art. 28 (9) **Form**	The contract or other legal act within the meaning of Art. 28 (3) and (4) GDPR must be concluded in writing, which may also take electronic form.	

1 EDPB Opinion 22/2024, para. 41; EDPB Guidelines 07/2020, para. 95.

2 EDPB Opinion 22/24, para. 42; EDPB Guidelines 07/2020, para. 99.

3 EDSA Opinion 22/24, para. 39.

4 Cf. Guidelines 07/2020, para. 94 ff.

5 EDSA Opinion 22/2024, paras. 37, 38.

2.7 Art. 30: records of processing activities

2.7.1 Introductory remarks

The criteria specified in Art. 30 are mainly examined based on whether the records of processing activities are complete. The records also contain a number of (partial) results from other processes that have to be considered under separate examination criteria. For example, the purposes of processing [point (b) of Art. 30 (1)] or technical and organisational measures [point (g) of Art. 30 (1)] cannot only be determined when maintaining this record; this must have been done beforehand.

When examining the records, special attention is paid to the processes within the controller's organisation that help to maintain the records as a "living" document, constantly and truthfully reflecting the current status of processing activities.

The special circumstances surrounding small businesses and micro-enterprises are also taken into account, as the requirement to keep records of processing activities may not apply and is therefore checked in advance (cf. Recital 13).

2.7.2 Tabular overview: requirements, forms of implementation and examination methods

Legal criteria	*Aspects to be covered by the certification criteria and implementation by the customers of the certification body*	*How will the certification body verify implementation?*
Art. 30 (5) Records of processing activities	The following requirements must be checked:	The certification body will determine the number of employees by conducting a survey or checking the

are necessary.	- number of employees and, if applicable, either - a risk to the freedoms and rights of natural persons; - not just occasional processing; or - processing of special categories of data pursuant to Art. 9 (1) or Art. 10.	relevant documents. The certification body will examine the legal, technical and organisational aspects of an assessment of processing activities to be carried out by the controller with regard to - the risk of processing; - the frequency of processing; and - the categories of personal data involved.
Art. 30 (1) Records are complete.	The records of processing activities must contain all the information specified in points (a) to (g) of Art. 30 (1). There must be processes in place for updating the records in the following cases: - if new processing activities are introduced; - if certain processing activities are no longer carried out; or - if any of the information to be provided under points	The certification body will examine the documents related to the records of processing activities. The certification body will examine written process descriptions and audit the relevant processes.

	(a) to (g) of Art. 30 (1) changes for processing activities that are already listed in the records. There must be processes in place to facilitate cooperation in this area between - the departments involved in the processing activities; - the controller's representative; and - the data protection officer, if applicable. The relevant responsibilities must have been clarified within the organisation.	The certification body will examine the following documents: - written process descriptions; - organisation charts; - business / task allocation plan; and - if necessary, questions posed to the controller.
Art. 30 (2) Records contain information for processors.	The records of processing activities must contain all the information specified in points (a) to (d) of Art. 30 (2). There must be processes in place for updating the records in the following cases:	The certification body will examine the documents related to the records of processing activities. The certification body will examine written process descriptions and audit the relevant processes.

	- if new categories of processing activities are introduced for processors; - if categories of processing activities assigned to processors are no longer carried out; - if any of the information to be provided under points (a) to (d) of Art. 30 (2) changes for categories of processing activities that are already listed in the records; - if processors start working for additional controllers; - if processors stop working for certain controllers; or - if any of the information specified in points (a) to (d) of Art. 30 (2) changes for existing controllers.	
	There must be processes in place to facilitate cooperation in this area between - the departments involved in the processing activities; - the representative of the controller acting as a processor;	The certification body will examine the following documents: - written process descriptions; - organisation charts; - business / task allocation plan; and - if necessary, questions posed to the controller.

	- if applicable,data protection officer of the controller acting as a processor; and - the controllers for whom processing is carried out. The relevant responsibilities must have been clarified within the organisation.	
Art. 30 (3) The records are kept in writing.	The records must be kept in writing. The storage locations must be known to the persons involved.	The certification body will examine the relevant documents.
Art. 30 (4) The records are made available to the supervisory authority upon request.	There must be processes in place to ensure that the following is done in a timely manner when a corresponding request is made by a supervisory authority: - the request is received; - the request is processed; and - a response is returned (providing the records of processing activities).	The certification body will examine the following documents: - written process descriptions; process audits; - organisation charts; - business / task allocation plan; and - if necessary, questions posed to the controller.

	The relevant responsibilities must have been clarified within the organisation.	

2.8 Art. 32: security of processing

2.8.1 Introductory remarks

Art. 32 stipulates that appropriate technical and organisational measures have to be implemented to protect personal data. In order to check whether this requirement has been met, the relevant measures and processes must be documented and the documentation must be available for review. The measures and processes must also be technically or physically accessible so that appropriate examinations can be performed to evaluate their functionality. When defining the technical and organisational measures, the level of security to be ensured is the central criterion for determining their appropriateness. The level of security must also be documented and continuously reviewed.

Certain requirements resulting from Art. 32 may be fully or partially met by suitable (IT security) certifications (e.g. ISMS according to ISO 27001, BSI Basic Protection) that also cover data protection aspects, cf. DSK supplementary paper.[19] If the relevant data protection requirements are met by one or more (IT security) certification(s), the extent to which the requirements have been completely and correctly satisfied must be checked and documented. A data protection requirement will be deemed to have been completely and correctly satisfied if it can be clearly matched to one or more requirements of an (IT security) certification and if the examination methods required for the (IT security) certification also correspond to the relevant data protection examination methods.

2.8.2 Tabular overview: requirements, forms of implementation and examination methods

Legal criteria	*Aspects to be covered by the certification criteria and implementation by the customers of the certification body*	*How will the certification body verify implementation?*
Art. 32 (1) and (2) The level of security is deter-	a) There must be a complete and detailed description of all processed data or categories of data.	The certification body will examine the relevant documents and question the controllers.

19 However, such certifications will only be recognised if they are issued by accredited certification bodies under the conditions listed in Section 7.4 of the DSK supplementary paper ("Accreditation requirements pursuant to Art. 43 in conjunction with DIN EN ISO/IEC 17065", available (in German) here: https://www.datenschutzkonferenz-online.de/media/ah/20201008_din17065_Ergaenzungen_deutsch_nach_opinion.pdf).

mined for all necessary processing activities.	b) A level of security must be established that is appropriate to the risk involved in processing (particularly taking into account Recitals 38 and 75).	The certification body will check whether the risk assessment method is GDPR-compliant. The certification body will examine the following document(s): risk assessment check (e.g. according to SDM D3). The certification body will examine the relevant documents and conduct legal analysis to check whether the resulting level of security satisfies the security requirements of the categories of data to be processed.
	c) Account must be taken of the risks presented by processing, in particular from the destruction, loss, alteration or disclosure of personal data or unauthorised access to personal data pursuant to Art. 32	The certification body will take the same approach as for b) but with a focus on the destruction, loss, alteration or disclosure of data or unauthorised access to data.

	(2).	
Point (a) and (b) of Art. 32 (1) Measures to protect personal data.	a) Measures must be taken to ensure the confidentiality of personal data (in particular pseudonymisation and encryption).	The certification body will examine the following document(s): specifications and security concepts, in particular with regard to the state of the art and the consistency of each measure. The certification body will examine the following document(s): comparison of the level of security ensured by the measures with the security requirements specified in Art. 32. The certification body will conduct on-site inspections, validation audits and interviews to appropriately verify whether the measures are being implemented. (The verification process will be deemed appropriate if one can assume that all measures are being implemented according to the concept / specifications. This

		may include audits of technology and processes, e.g. penetration / stress tests, and audits according to common technical standards, e.g. BSI Basic Protection or ISO 27001).
	b) Measures must be taken to ensure the achievement of other objectives under the GDPR and/or SDM C1 for personal data (depending on the level of security needed to mitigate the risk).	See a).
	c) Customers must document their processes used to select and implement suitable technical and organisational measures in a way that ensures the confidentiality, integrity and availability of processing (key objective: availability, integrity and confidentiality, cf. Art. 5).	Document check, methodological analysis: The certification scheme must at least require the certification body to check the technical and organisational measures to ensure that the requirements for ensuring availability, integrity and confidentiality are met.
Point (b) of Art. 32 (1) Measures to protect systems and services on an ongoing basis.	a) Measures must be taken to ensure the achievement of other objectives under the GDPR and/or SDM C1 to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services.	The certification body will examine the following document(s): specifications and security concepts, in particular with regard to the state of the art and the consistency of each measure (authorisation concept, identity management,

		authentication, authorisation, auditing and logging concept). The level of security ensured by the measures must correspond to the security requirements for the overall system (e.g. according to IT security concept). The certification body will verify this by comparing the two factors. The certification body will conduct on-site inspections, validation audits and interviews to appropriately verify whether the measures are being implemented (see above).
	b) The measures specified in a) must be ensured on an ongoing basis.	The certification body will examine the relevant documents and conduct interviews to check the business continuity concept, e.g. according to BSI 200-4 or ITIL (in particular checking whether the relevant systems are fully covered and verifying compliance with the PDCA principle / Deming circle). The certification body will conduct on-site inspections,

		validation audits, unannounced visits and interviews to verify whether the relevant management processes have been implemented (e.g. by simulating internal and external incidents such as intentional attacks and unintentional events and/or by carrying out load tests).
Point (c) of Art. 32 (1) Measures to ensure the availability of personal data in regular operations and in the event of incidents.	a) Measures must be taken to ensure the availability of personal data in regular operations.	The certification body will examine the following document(s): specifications and the relevant concepts (e.g. review of availability levels, service level agreements), in particular with regard to the state of the art. The level of availability ensured by the measures must correspond to the availability requirements for the processed personal data; this must be appropriate to the risk involved, as determined in accordance with Art. 32 (1). The certification body will verify this by comparing the two factors.

		The certification body will conduct on-site inspections, validation audits and interviews to appropriately verify whether the measures are being implemented (e.g. according to ITIL Availability Management, KRITIS).
	b) Availability must be ensured in the event of physical or technical incidents.	The certification body will examine the following document(s): availability and disaster recovery concepts (e.g. according to ISO 2700x). The certification body will conduct on-site inspections, validation audits, unannounced visits and interviews to verify the measures and processes contained in the concepts mentioned above (e.g. by simulating internal and external incidents such as intentional attacks and unintentional events and/or by carrying out load tests) in relation to personal data.
Point (d) of Art. 32 (1)	a) A process must be in place to ensure that all relevant	The certification body will conduct validation audits for

A process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures.	systems and processes are regularly tested, assessed and evaluated to verify the effectiveness of technical and organisational measures. b) The measures established in a) must be correctly (effectively) implemented for all systems and processes.	each management system (e.g. ISMS, ITIL Service Continuity Management) and each monitoring system and process (e.g. Incident response, CERT, IDS/IPS). See a).
Art. 32 (4) Measures to ensure that any natural persons acting under the authority of controller(s) or processor(s) only process personal data when instructed to do so.	There must be arrangements in place for the processing of personal data, and these must be correct.	The certification body will examine documents and conduct legal analysis to determine whether the relevant company policies and arrangements are lawful and correct. The certification body will examine the relevant documents and conduct interviews to check whether the company policies and arrangements are consistent with each controller's organisational structure.

2.9 Art. 33 and 34: notification of a personal data breach to the supervisory authority and communication of a personal data breach to the data subject

2.9.1 Introductory remarks

Art. 33 and Art. 34 contain provisions regarding the notification of the supervisory authority and data subjects in the event of a personal data breach.

Specifically, those articles detail the necessary content and deadline of such notifications, the relevant documentation obligations and duties, as well as possible exceptions to the notification requirement.

2.9.2 Tabular overview: requirements, forms of implementation and examination methods

Legal criteria	*Aspects to be covered by the certification criteria and implementation by the customers of the certification body*	*How will the certification body verify implementation?*
Art. 33 Obligation to report personal data breaches to the supervisory authority.	There must be a process in place to regulate how personal data breaches are to be handled from an operational perspective to meet the reporting requirements. As part of this process, specific	The certification body will check whether and to what extent procedures / processes have been established to deal with data protection incidents and make everyone

	procedures and responsibilities must be defined and all those involved must be made aware of general principles related to the detection of data breaches.	involved aware of general principles related to the detection of data breaches. These checks may come in the following forms: - document check; - on-site inspection; and/or - interviews with employees.
First sentence of Art. 33 (1) Personal data breach.	Any "personal data breaches", as defined in Art. 4 No. 12, must be identified, analysed and evaluated.	See above.
First sentence of Art. 33 (1) Exemption from reporting if a personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.	The risk must be identified, analysed and evaluated (see "data protection risk assessment").	See above.
First sentence of Art. 33 (1) Deadline ("without undue delay	Measures must be taken to meet deadlines, to identify any delays, if necessary, to justify them.	See above.

and, where feasible, no later than 72 hours”). Second sentence of Art. 33 (1) Obligation to state reasons for any delays.		
Art. 33 (2) Processor’s obligation to notify the controller.	Measures must be taken to ensure that the processor notifies the controller of any personal data breaches (e.g. provision in data processing agreement).	See above (particularly including an examination of the data processing agreement).
Art. 33 (3) Content of notification.	There must be measures in place to ensure that all the relevant details of a personal data breach are reported, using notification forms provided by the supervisory authority if necessary.	See above.
Point (d) of Art. 33 (3) Measures to address the breach including, if appropriate, measures to mitigate its potentially adverse effects.	The relevant technical and organisational measures must be adopted and implemented. The focus of such measures should be on identifying, analysing and evaluating the personal data breach and the risk (see above).	See above.
Exception with regard to the	Any information that cannot be provided at the same	See above.

content of notifications: Art. 33 (4) Provision of information in phases.	time must be provided in phases pursuant to Art. 33 (4). The deadline pursuant to the first second sentence of Art. 33 (1) must still be observed if the minimum information specified in Art. 33 (3) cannot be provided at the same time within the deadline. In such cases, the necessary content / scope of the notification may be provided in phases, but the information must actually be made available in phases for the deadline to be met (initial and subsequent notifications). Measures must be taken to ensure that the deadline is met and that the necessary information is subsequently provided (in phases).	
First sentence of Art. 33 (5) Documentation requirement.	All personal data breaches must be documented, including the facts relating to the breach, its effects and the remedial action taken. The documentation must enable the supervisory authority to verify compliance with the provisions of Art. 33.	See above.

Art. 34 Obligation to communicate personal data breaches to data subjects.	There must be a procedure in place to regulate how personal data breaches are to be communicated to data subjects in such a way that the requirements are met. As part of this process, specific procedures and responsibilities must be defined.	The certification body must be able to check the procedures / processes (cf. Art. 33).
Art. 34 (1) Personal data breach likely to result in a high risk.	See above for Art. 33	
Art. 34 (1) Deadline.	See above for Art. 33	
Art. 34 (2) Content of notification.	See above for Art. 33	
Art. 34 (3) Exemption from notification re-quirement.	An examination must be conducted to check for any exemptions.	
Art. 34 Documentation of compliance	The documentation must enable the supervisory authority to verify compliance with the provisions of Art.	

with requirements.	34.	

2.10 Art. 35: data protection impact assessment

Legal criteria	*Aspects to be covered by the certification criteria and implementation by the customers of the certification body*	*How will the certification body verify implementation?*
Art. 35 Assessment of necessity	The controller must conduct a data protection impact assessment (DPIA) if there is likely to be a high risk when the subject of certification is used within its scope of application (the controller will usually decide whether a DPIA is necessary based on the **description of the planned processing operations** and the respective purposes of processing; it is therefore crucial that the controller creates records of processing activities in accordance with Art. 30). For this purpose, the controller must check whether at least one processing operation covered by the subject of	The certification body will examine the relevant documents and may also conduct interviews. The controller and processor must document and explain the examination results specifically related to the DPIA for the use of the subject of certification within its scope of application. Optional: A sample DPIA may be examined for the use of the subject of certification in one or more context; this will be specified by the controller or processor according to their own use of the subject of certification.

	certification is included in one of the following lists: - the special requirements listed in Art. 35 (3); - the list described in Art. 35 (4) (whitelist); or - the list described in Art. 35 (5) (blacklist). The controller must also check whether a DPIA has to be carried out for the subject of certification for any other reasons, e.g. because - the processing of personal data meets the EDPB's current criteria (e.g. WP 248); or - a DPIA is required by federal, state or special legislation.	
Art. 35 Minimum requirements	The formal requirements for conducting a DPIA are specified in the GDPR, specifically in Art. 35 and Recitals 84, 90, 91, 92 and 93. The controller will generally be free to choose an appropriate method.	The certification body will examine the relevant documents and may also conduct interviews. The controller and processor must document and explain the outlined requirements for the use of the subject of certification within its scope of application.

	The GDPR does not contain any explicit formal requirements for conducting a DPIA. However, a list of minimum contents can be found in Art. 35 (7): - a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller; - an assessment of the necessity and proportionality of the processing operations in relation to the purposes; - an assessment of the risks to the rights and freedoms of data subjects referred to in Art. 35 (1); and the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to	Optional: A sample DPIA may be examined for the use of the subject of certification in one or more contexts; this will be specified by the controller or processor according to their own use of the subject of certification. Note on high residual risks: If a DPIA indicates a high risk to the rights and freedoms of natural persons despite technical and organisational measures being taken to mitigate the risk (i.e. a residual risk), the controller must consult the competent supervisory authority in accordance with Art. 36.

	demonstrate compliance with the GDPR [on an on-going basis[20]], taking into account the rights and legitimate interests of data subjects and other persons concerned.	

2.11 Art. 44 *et seq.*: transfer of personal data to third countries

2.11.1 Introductory remarks

If the subject of certification involves the transfer of personal data to third countries or international organisations (hereinafter referred to collectively as “data transfers to third countries”), the legal requirements specified in Art. 44 to 49 must be observed to make sure that such data transfers to third countries are lawful. A certification scheme must therefore examine whether the subject of certification includes data transfers to third countries and whether such data transfers are legally permissible.[21]

This results in the following mandatory content (i.e. certification criteria) for certification schemes:

1. Are data transfers to third countries ruled out?

20 A DPIA is not a one-time process; it must be carried out again if there are changes in risk or significant changes in the process. In this respect, an iterative process of reviews and adjustments is recommended.

21 For certification as tools for transfers pursuant to point (f) of Art. 46 (2), see “Guideline on certification as tools for transfers” (add no. after EDPB plenary session).

The certification body must first examine whether data transfers to third countries can be ruled out within the scope of the subject of certification. In doing so, the certification body should bear in mind that data is often transferred to third countries for maintenance, care and support purposes. The relevance of such transfers is often overlooked, especially when the subject of certification does not revolve around maintenance, care and support services or the transfers are not usually planned but necessary in exceptional cases. For this reason, certification bodies and scheme owners must also take into account such services and the activities of any sub-processors when examining the extent to which data transfers to third countries can be ruled out; this must be specifically included in the scope of their certification scheme.

2. Two-stage check

If data transfers to third countries cannot be ruled out for the subject of certification, the certification body's customers must check and document the legal basis on which personal data is transferred to third countries (and the certification body must then examine the documentation provided). A two-stage check must then be conducted to determine and document (1) whether, notwithstanding the specific requirements for data transfers to third countries pursuant to Chapter 5 GDPR, the other provisions of the GDPR are observed with regard to the processing in question; and (2) the extent to which the specific requirements of Art. 44 to 49 are observed.

In the second stage, customers are especially expected to present, examine and document the basis on which personal data is transferred to third countries. Furthermore, specific scenarios[22] must be created for additional guidance. The scenarios should be integrated into a methodology that allows the subject of certification to be evaluated in a comprehensible, reliable and reproducible manner.

The following should be considered as a possible legal basis for data transfers to third countries:

1. an adequacy decision of the Commission pursuant to Art. 45 (1) and (3); or
2. appropriate safeguards pursuant to Art. 46 (1), if applicable in conjunction with Art. 47[23].

The publications of the data protection supervisory authorities at national and European level should be taken into account in each case, as well as developments in relation to the determination of the adequate level of security and case law (e.g. the "Schrems II" judgement of the CJEU).[24]). As a general rule, Art. 49 cannot be considered as the legal basis for recurring data transfers to a third country.[25]

---

22 For this purpose, the EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data should be consulted and the cases described in that document should be specified in greater detail where necessary.

23 This also includes binding corporate rules pursuant to Art. 47, standard contractual clauses adopted by the Commission, standard data protection clauses adopted by a supervisory authority, and approved codes of conduct pursuant to Art. 40.

24 Judgement of the European Court of Justice of 16 July 2020 (Case C-311/18).

25 Guidelines 2/2018 on derogations of Art. 49 under Regulation 2016/679, adopted on 25 May 2018, p. 4.

2.11.2 Examination steps

There are two possible scenarios:

1. The data is exported by the controller: The controller must comply with the requirements specified in Chapter 5 of the GDPR.
2. The data is exported by the processor: The processor must comply with the requirements specified in Chapter 5 of the GDPR. However, the controller must at least incidentally check the requirements specified in Chapter 5 of the GDPR pursuant to Art. 28 (1) and point (a) of Art. 28 (3).

Examination criteria	*Aspects to be covered by the certification criteria and implementation by the customers of the certification body*	*How will the certification body verify implementation?*
Awareness of planned data transfers	All processing activities involving the transfer of personal data to a third country must be presented and documented. The presentation must show which types of data are affected, which third countries are involved (also in transit) and which technologies are used.	The certification body will examine the relevant charts and documents, in particular those related to the controller's obligation to provide information under Art. 13 and 14. It will also examine records of processing activities pursuant to Art. 30. Furthermore, the certification body will examine the

		planned and used services and their actual data flows[26].
Examination of an appropriate transfer tool (pursuant to Art. 44)	The transfer tools selected from Art. 45 and 46 must be presented in addition to the examination that led to that selection. a) Adequacy decision issued by the European Commission for the target country If an adequacy decision has been issued, it must be regularly reviewed to ensure that it is still in place and an emergency plan must be drawn up if it is ever revoked. If there is no adequacy decision, point b) and the other points in the table must be examined. b) Transfers based on a transfer tool pursuant to points (a) to (f) of Art. 46 (2) or point (a) or (b) of Art. 46 (3),	The certification body will examine the relevant documents (incl. process descriptions).

26 E.g. third-party providers on websites, hosting providers, content delivery networks, Internet security services, geo-location services, customer relations management systems.

	each in conjunction with Art. 46 (1) (enforceable rights and effective remedies).	
Further examination in the absence of an adequacy decision Assessment of legal situation and practice in the target country.	The level of protection for personal data in the third country[27] must be compared with the level of protection within the geographical scope of the GDPR. Any facts that might cause the level of protection in the target country to be deemed lower than in the EU or the EEA, meaning that transfers are only permitted with supplementary measures, must be identified. Evidence must be provided to prove that an adequate level of protection is ensured when using the selected transfer tool for the specific subject of certification[28]. The analysis of the legal situation and practice in the target country must meet the criteria laid down in Recommendations 01/2020, and the level of protection must meet the requirements of Recommendations	The certification body will examine the relevant process descriptions and conduct a legal review of the documentation and the legal situation and practice in the third country based on the (not exhaustively listed) sources of information pursuant to Annex 3 of Recommendations 01/2020.

27 In practice, it is worth limiting the subject of certification to specific third countries, whose legal situation has to be assessed and monitored in each case.
28 Judgement of the European Court of Justice of 16 July 2020 (Case C-311/18).

	02/2020 on the European Essential Guarantees for surveillance measures.	
Selection and application of supplementary measures.	There must be processes in place to select suitable supplementary measures within the scope of the scenarios presented by the EDPB[29] based on the gaps identified with regard to the protection of personal data in the target country (incl. any transit countries and stops along the way). If supplementary measures are possible, they must be implemented in the form of the measures presented in EDPB's scenarios[30].	The certification body will examine the relevant documents and the technical and organisational measures (pseudonymisation, encryption).
Complementary measures taken by the data importer	There is a basic assumption that any supplementary measures taken by the data exporter must be appropriate (and effective) in the importer's specific circumstances. In particular, an examination must be carried out to check whether any supplementary	The certification body will examine the relevant process descriptions and documents. The data processing agreement or written instructions will be presented to the certification body.

29 Cf. Annex 2 of Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data.

30 Cf. Annex 2 of Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data.

	measures are required from the importer and whether corresponding instructions have been issued regarding additional measures to be taken by the importer. If certification pursuant to point (f) of 46 (3) is chosen as the transfer tool, the requirements for the effectiveness of the supplementary measures pursuant to "GL Certification as tools for transfer"[31] must also be met. This means that an examination must be carried out to check whether the importer's certificate matches the exporter's data and scenarios.	The certification body will check whether the instructions are implemented by the importer. The importer's certificate will be submitted to the certification body.
If applicable, formal procedures	In the cases described in Art. 46 (3), the competent supervisory authority must be involved for authorisation purposes.	The certification body will examine the relevant process descriptions and documents.
Regular monitoring and re-	There must be processes in place to ensure that the	The certification body will examine the relevant process

31 Cf. point 3.2.7 of GL: Additional safeguards concerning the exporter and Annex I to the Guidelines on certification as tools for transfers (draft as of May 2022).

evaluation	development of the legal situation and practice in the third country can be regularly evaluated in conjunction with the relevant effects on the level of protection for personal data; there must be an emergency plan in case the level of protection falls.	descriptions and documents. The certification body will inspect and verify implementation as described in the previous steps.

2.12 Rights of data subjects

The following rights of data subjects must be seen as mandatory certification criteria to be included in a certification scheme:

1. transparency and means of exercising the rights of data subjects pursuant to Art. 12;
2. obligation to provide information when collecting personal data pursuant to Art. 13 and 14;
3. right of access pursuant to Art. 15;
4. right to rectification pursuant to Art. 16;
5. right to erasure ("right to be forgotten") pursuant to Art. 17;
6. right to the restriction of processing pursuant to Art. 18;
7. obligation to notify data subjects in relation to the rectification or erasure of personal data or the restriction of processing pursuant to Art. 19;
8. right to data portability pursuant to Art. 20;
9. right to object pursuant to Art. 21; and
10. automated individual decision-making, including profiling, pursuant to Art. 22.

If any of the points listed above are not relevant for the subject of certification under consideration, reasons must be given as to why it is not necessary for the specific subject of certification.

3 Processes during the certification validity period

In order for a certification scheme to be used, the relevant criteria must first be approved by the competent independent supervisory authority. For this purpose, processes surrounding the subject of certification must be defined and implemented, and organisational measures must be taken. These processes must be embedded within data protection management to ensure that the GDPR conformity of the subject of certification is maintained for as long as the data protection certification remains valid. In other words, these processes perform a sort of dual function when it comes to data protection certification: On the one hand, they form part of the organisation's data protection management; on the other hand, from a certification perspective, they form an integral part of the subject of certification. As such, they are the subject of the data protection examination and assessment to be conducted by the certification body during the certification process and are therefore included in the certification granted, but only to the extent that they relate to the subject of certification. The organisation's entire data protection management is not certified here.

In order to ensure an adequate examination and the long-term functionality of these processes, and thus also a valid and verifiable seal statement that lasts throughout the certification validity period, clearly separate competencies and responsibilities must be defined and guaranteed in this context. For this purpose, the tasks of the certification body and the holder of a data protection seal or quality mark must be clearly distinguished from one other. They must be presented in such a way that both the competencies and responsibilities of the respective certification body and the holder of a data protection seal or quality mark are clearly evident.

The data protection processes to be certified include at least the following processes:

- administrative processes specifically related to data protection that describe the relationship between the certification body and the holder of a data protection seal or quality mark (e.g. ensuring that contact details are provided for specific points of contact on both sides, including their authorisations);

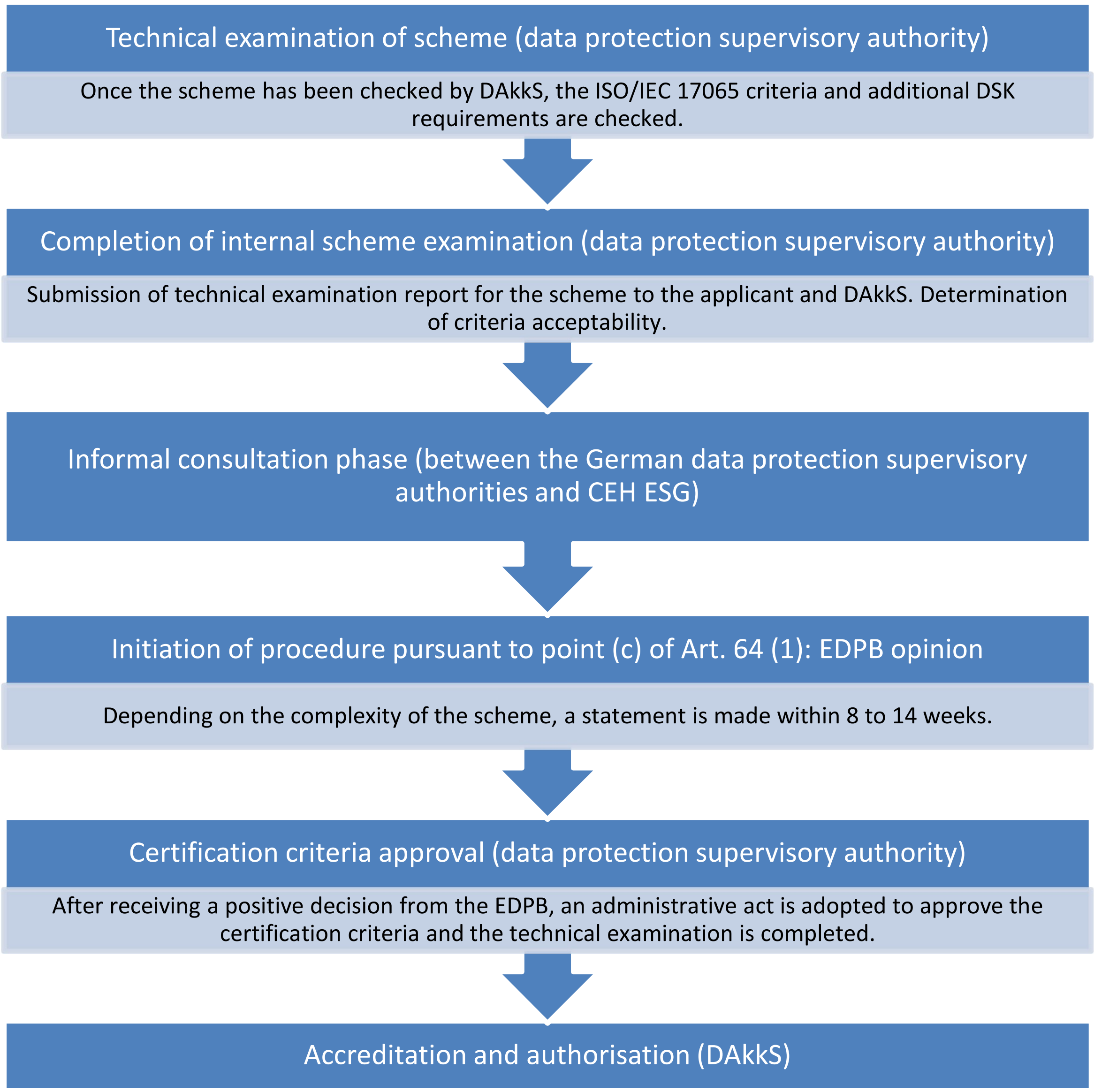
- processes for ongoing compliance with data protection principles pursuant to Art. 5;
- processes specifically related to data protection to protect the rights of data subjects pursuant to Art. 12 to Art. 22;
- processes for data protection risk assessments pursuant to Art. 30 in conjunction with Art. 35 and 36;
- processes for dealing with personal data breaches pursuant to Art. 33 and 34
  - with identification, analysis, technical evaluation and legal review of the associated risks of personal data breaches affecting the owner of a data protection seal or quality mark; and
  - with the subsequent selection and implementation of technical and organisational measures pursuant to point (d) of Art. 33 (3);
- implementation of technical and organisational measures from a process perspective, which can be controlled and monitored using IT-based processes if necessary and are to be implemented taking into account and applying Art. 25 and 32; and
- presentation of the valid, process-based transformation of data protection requirements into systems and services for which a suitable and appropriate form of technical assessment must be ensured and a (recurring) legal assessment must be guaranteed.[32]

32 Such an assessment of the processes derived from the transformation of the data protection requirements must also be presented in the certification scheme. The SDM may serve as a starting point for understanding such transformations (cf. https://www.datenschutz-mv.de/datenschutz/datenschutzmodell/).

4 Workflows for German and European data protection seals

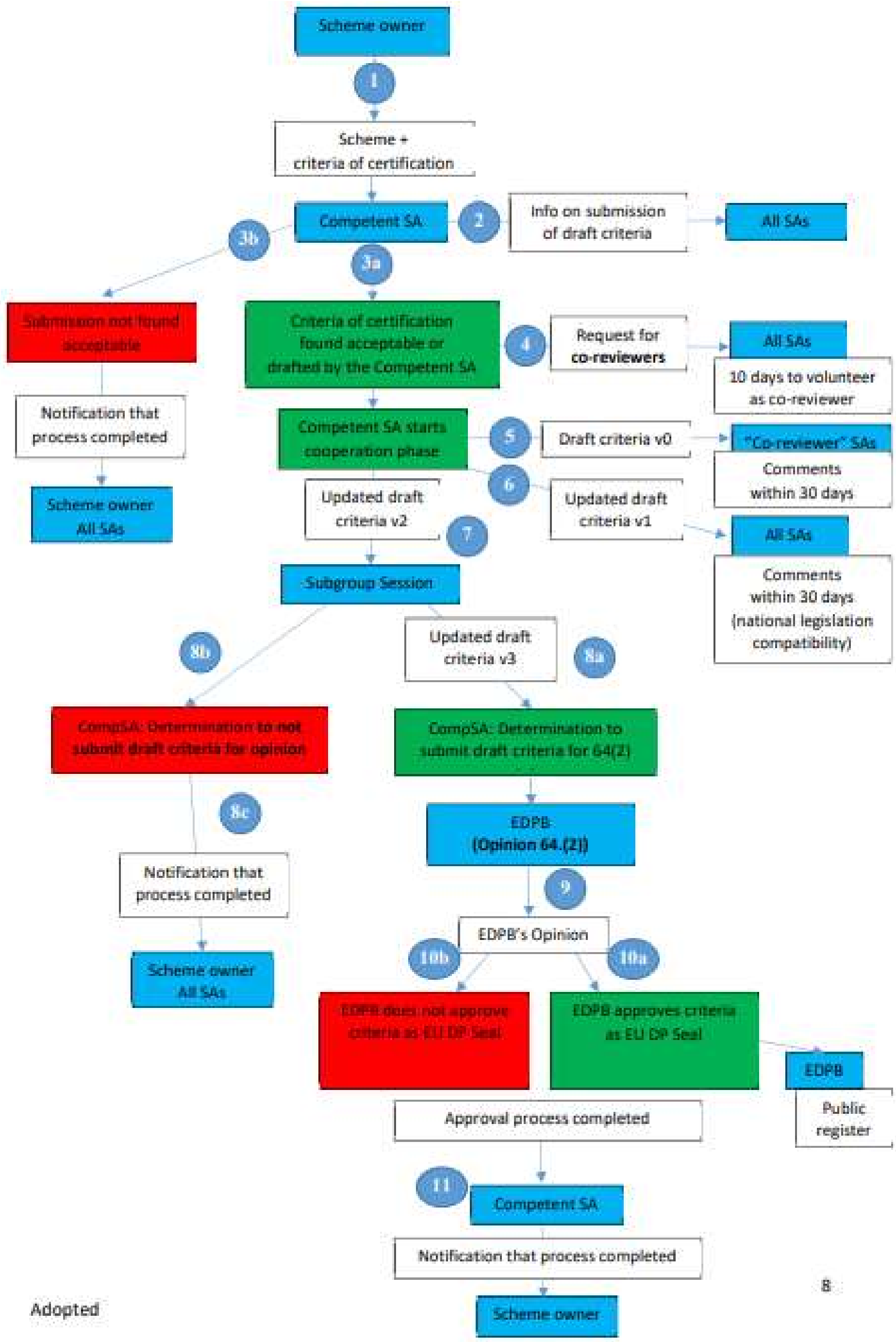
4.1 Workflow: approval of German data protection seal

The following chart presents the further procedure for awarding seals in Germany:



4.2 Workflow: approval of EU data protection seal

Here is an illustration of the further procedure observed by the EDPB when it comes to approving certification criteria leading to a European data protection seal (new version of the illustration expected for beginning 2023).



Source: https://edpb.europa.eu/our-work-tools/our-documents/procedure/edpb-document-procedure-approval-certification-criteria-edpb_de

5 List of abbreviations / glossary

AkkStelleG	German Accreditation Body Act
Art.	Article
BDSG	German Federal Data Protection Act
BSI	Federal Office for Information Security
CERT	Computer Emergency Response Team
DAkkS	Deutsche Akkreditierungsstelle GmbH
DPIA	Data protection impact assessment (Art. 35 GDPR)
DSK	Datenschutzkonferenz
EDPB	European Data Protection Board
GDPR	General Data Protection Regulation
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
ISMS	Information Security Management System
ITIL	Information Technology Infrastructure Library
KRITIS	Critical infrastructure
PDCA principle	Plan-Do-Check-Act, Deming circle
SDM	Standard Data Protection Model
TFEU	Treaty on the Functioning of the European Union

A glossary can be found (in German) in Annex 1 to the DSK supplementary paper on "Accreditation requirements pursuant to Art. 43 (3) GDPR in conjunction with DIN EN ISO/IEC 17065".