# Data protection requirements

## certification programs

Data protection test criteria, test system and test methods for adapting

Solution and application of the technical standard DIN EN ISO/IEC 17067 (program type 6)

Version 1.8 (04/16/2021)

O -	- 4 -	4 -
Co	nto	nte
$\sim$		HILO

Objective and classification	
1.1	
1.2	
1.3	
Goal	
Classification in the control system	
Test procedure 4	
1.4 Basic documents	5
2	
Certification criteria and requirements for a certification object	
2.1 Basic requirements	
2.1.1 Description of the subject of certification	
2.1.2 Information from the applicant on the object of certification	
2.1.3 Compliance with the relevant data protection regulations	
2.2 Article 5: Principles governing the processing of personal data	
2.3 Article 6: lawfulness of processing	
2.4 Article 25: Privacy by design and by privacy-friendly	
Presets	
2.5 Article 28: Processors	

2.5.2

Introductory notes
Tabular overview: requirements, forms of implementation and testing 23
2.6 Article 30: Record of processing activities
2.6.1
2.6.2
Introductory notes
Tabular overview: requirements, forms of implementation and testing 26
2.7 Article 32: Security of processing
2.7.1
2.7.2
Introductory notes
Tabular overview: requirements, forms of implementation and testing. 30
2.8 Articles 33 and 34: Notification of personal data breaches
the supervisory authority and notification of the person affected by a breach 36
2.8.1
2.8.2
Introductory notes
Tabular overview: requirements, forms of implementation and testing 36
2.9 Article 35: Data protection impact assessment
2.10
2.11
Data transfer to third countries or to internal organizations
Rights of data subjects42
Processes during the validity period of the certification

List of abbreviations/Glossary .......45

3

4

1 Objective and classification

#### 1.1 Objective

To prepare for an accreditation, the certification body or the program owner must

Create certification program and check for suitability by DAkkS1 in accordance with DIN EN ISO/IEC 17011

(cf. DAkkS rule 71 SD 0016). An essential part of this certification program are the tification criteria for the implementation of data protection requirements. These are acc.

Article 57 paragraph 1 lit. n GDPR i. In conjunction with Art. 42 (5) GDPR2 either by the responsible data protection supervisory authority or (usually via the competent supervisory authority) the European submitted to the Data Protection Committee for approval or approval in accordance with Articles 63, 64 (1) (c).

This document describes the minimum requirements for the certification criteria that

fulfilled by all certification programs in addition to the requirements of DIN EN ISO/IEC 17067 have to be. Due to the specifics of a certification program, further requirements may arise gene.

A certification program must therefore necessarily meet the following requirements for certification contain:

- (1) The requirements from DIN EN ISO/IEC 17067 (program type 6);
- (2) the minimum requirements for all certification programs from the present the document:
- (3) if necessary, special requirements: These can be e.g. B. it follows that a certification program is focused on a specific area, specific processing ment processes addressed or potential certification objects in the application rich in special legal regulations.

Further requirements can be made by the accreditation bodies, in particular taking into account

the guidelines of the European Data Protection Board (EDPB)3, the decisions of the conference the independent data protection supervisory authorities of the federal and state governments, case law or of the accreditation practice.

For the above reasons, this document does not claim to be complete.

It is intended to be used by the German supervisory authorities when evaluating certification programs as a serve as a uniform basis for evaluation and program owners and certification bodies help to provide their documents as orientation.

1 The German Accreditation Body GmbH (DAkkS) has its legal basis in the Accreditation Body Act (AkkStelleG) according to EU-VO 765/2008.

2 Insofar as it concerns articles from the GDPR, the addition "GDPR" will be omitted in the further course.

3 See in particular "Guidelines 1/2018 for the certification and determination of certification criteria according to the articles 42 and 43 of Regulation (EU) 2016/679" https://edpb.europa.eu/our-work-tools/our-documents/leitlinien/guidelines-12018-certification-and-identifying-certification\_en.

1.2

Classification in the control system

The starting point for designing certification programs is DIN EN ISO/IEC 170674.

This standard does not contain any subject-specific aspects, so that the formulation of requirements

Data protection criteria in accordance with Article 42, paragraph 5, adjustments and additions to DIN EN ISO/IEC

17067 by the independent supervisory authorities.

The application of DIN EN ISO/IEC 17067 includes the definition and delimitation of various program types. Due to the data protection testing experience and practice in the responsible Supervisory authorities must establish certification programs for data protection seals and test marks in accordance with Art. 42 aligned with program type 6.

### 1.3 Testing Procedures

The certification program must provide for an assessment process that includes a practical assessment, a technical assessment and legal assessment of ongoing compliance with the requirements of

respective certification program (actuality). Result from the respective review ment, evaluation and assessment of the need for change, suitable measures must be taken accordingly grasp. This testing process must be implemented at the time of certification and for the be maintained and guaranteed for the entire period of validity.

In a certification program, in addition to the certification requirements mentioned under 1.1 to explain which test procedure an accredited certification body uses to objects checked.

The data protection test procedure must be suitable for the proper implementation of data intellectual property requirements and the effectiveness of technical and organizational measures for the object of certification compared to the specified approved criteria according to Article 42, paragraph 5 determine and prove. GDPR compliance is achieved when such evidence for the subject of certification is provided.

Every certification program must claim that a properly issued certificate

no objection in a data protection examination of the certification object

status by an independent supervisory authority. A certification program must therefore

be suitable for fully checking the GDPR conformity of the object of certification and

to prove. The supervisory authority may exercise its supervisory powers at any time and

e.g. B. come to the conclusion that data processing is illegal.

4 DIN EN ISO/IEC 17067 is the follow-on standard of DIN EN ISO/IEC 17065 in the application of technical standards, which Application in Art. 43 Para. 1 lit. b is stipulated by law.

#### 1.4 Base Documents

This document for the design of criteria according to Art. 42 Para. 5 with the associated test system tik and the associated test methods i. In conjunction with DIN EN ISO/IEC 17067 (program type 6) builds up

the requirements of Art. 43,

the aforementioned and topic-specific guidelines of the EDPB,

the standards ISO/IEC 17065 and ISO/IEC 17067 and

the supplementary paper of the DSK5 according to Art. 43 Para. in conjunction with DIN EN ISO/IEC 17065 for certification certifying bodies, which within the framework of the accreditation by the DAkkS in agreement with the competent independent supervisory authorities.

2 Certification Criteria and Requirements for a Certification subject

- 2.1 Basic requirements
- 2.1.1 Description of the subject of certification

The certification program must specify the processing activities for which it is to be used. the should. This defines the scope of the certification program. The application rich should only contain processing in the material and geographical scope of the GDPR ten.6

The minimum requirements for the certification programs according to 2.1.3 and 2.2 ff.

view. These must be certified by both the accredited certification body and the responsible

be checked by the data protection supervisory authority. If it is a generic certification

program, the data protection requirements are to be met prior to the implementation of a certification

fication and to have it checked for completeness by the certification body. The certi
certification program must provide that the certification of a processing activity of a ver
extends to all relevant processing steps that are carried out by the person responsible

themselves, in joint responsibility with another responsible person and everyone included

any processor including all sub-processors.

5 "Requirements for an accreditation according to Art. 43 i. V. m. DIN EN ISO/IEC 17065" at https://www.datenschutzkonferenz-online.de/media/ah/20201008\_din17065\_Ergaenzungen\_deutsch\_nach\_opinion.pdf.

6 Note: The controller/processor does not have to fall under the territorial scope of the GDPR

len, cf. Article 42 (2). B. the scope of Directive (EU) 2016/680 of the Euro-

European Parliament and Council of April 27, 2016 on the protection of natural persons with regard to the processing of personal

collected data by competent authorities for the purpose of preventing, investigating, detecting or prosecuting criminal offenses or the execution of sentences as well as the free movement of data and the repeal of the framework decision 2008/977/JHA of the Council ("JHA Directive") as compliance with the JHA Directive is not subject to certification Art. 42 can be.

2.1.2 Information from the applicant on the object of certification

Certification programs should contain specifications as to what information about the to be certified

Processing, i.e. the object of certification, the applicant of the certification body before

measures of the test procedure has to be submitted. The following information is, insofar as it relates to the respective processing

applicable, at least to require

- 1. Which processing operations are covered by the object of certification;
- which purposes are covered by these processing operations and why these processing operations are necessary to achieve the purpose;
- 3. Recipients or categories of recipients;
- 4. which data is processed in connection with the subject of certification and
- a. which of these data are special categories of personal data pursuant to Art. 9;
- b. which data relate to criminal convictions and offenses under Article 10;
- c. which data relate to children within the meaning of the GDPR;
- 5. who processors according to Art. 4 Para. 8 regarding which processing operations of the certification subject of the insurance;
- 6. whether with regard to certain processing operations of the object of certification a there is joint responsibility according to Art. 26;

- whether, with regard to the processing operations of the object of certification, a transmission development of personal data
- a. outside the European Union or the European Economic Area or
- b. to international organizations.

The data transmission can also be used in the context of administration, maintenance, care or support are available to verify the functionality of the object of certification during the period of validity subject to certification.

- 8. what the main and subcomponents are and how they are broken down (see also Realization of processing operations using systems and services), for example through

  The following points:
- a. List of all participants group formation enables summaries (e.g. customers, users and administrators, etc.);
- Representation of how the data flows, naming the data types between the components and participants are recorded;
- c. Consideration and, if necessary, explanation of legal bases for the processing of personal ment-related data in the (partial) components and in relation to the transmission data flows and data types.

The connection between the considered legal bases, technical standards and the object of certification depending on the specific use is in the certification gram comprehensible.

2.1.3 Compliance with relevant data protection regulations

Art. 42 para. 1 provides that certification procedures should serve to prove that the GDPR Processing operations are complied with by those responsible and processors. About this To achieve this goal, the respective certification criteria must guarantee that the entity Compliance with all relevant requirements of the GDPR is ensured.

Provide the EDPB's Guidelines 1/2018 on certification and on determining certification criteria7

an orientation in this context. These name aspects that are to be described in the certification program are considered. Since this paper is a document that is continuously terdeveloped, the articles of the GDPR listed in the following paragraphs viewed with different degrees of detail. This is not to be understood as an evaluation and serves just for illustration.

Insofar as a presentation in the form of tables is given in the following sections of this chapter, the statements made there are not conclusive. So are in addition to the listed test methods other assessment techniques are possible. The test methods should be based on the standards oriented evaluation methods, e.g. B. Audit according to ISO 17021, testing according to ISO 17025 or Inspection according to ISO/IEC 17020.

In this version of the document, the requirements for the international

Data transfer and the rights of the data subjects regulated in Chapter 2.11 (Articles 12 to 23) initially presented only in general terms, without formulating the specific minimum requirements. last teres reserve the authors of this document for a subsequent edition.

2.2 Article 5: Principles governing the processing of personal data

Statutory facts

times

In the certification criteria too

audit topics to be dealt with and

ren implementation by the customers8

the certification body9

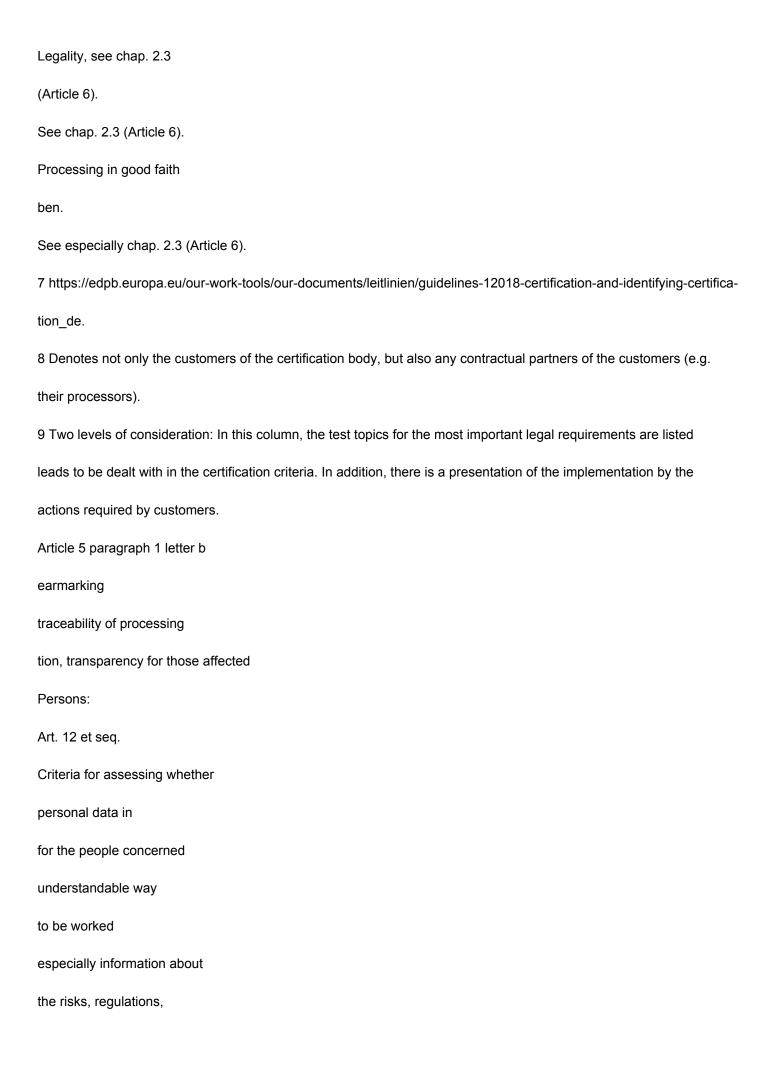
How does the certification

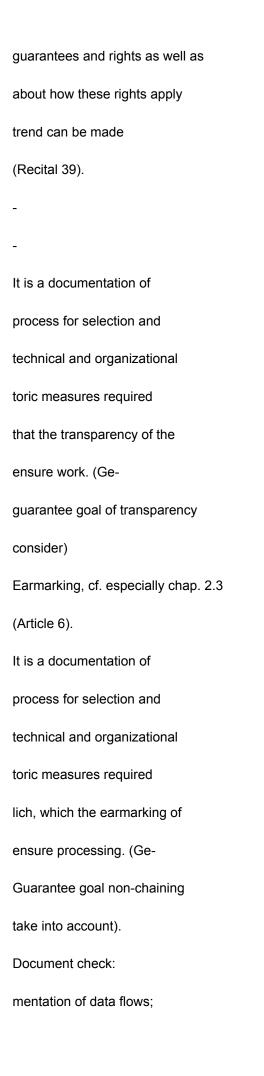
put the implementation?

Article 5 paragraph 1 letter a

Legality, Faithfulness and

belief, transparency

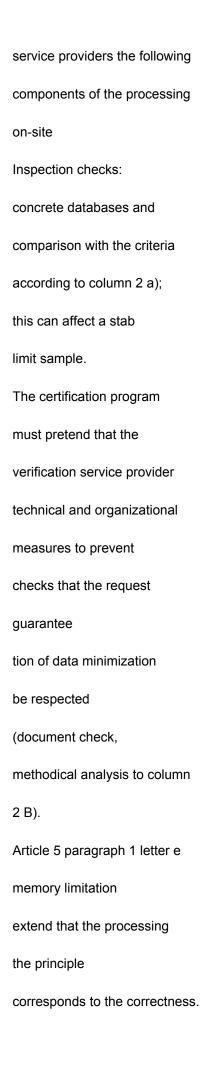




Directory of processing
activities; information
13, 14; Documentary-
mentation of the process for
Warranty and
preservation of transparency
for affected persons
to.
Inspection of all relevant
business processes and systems
teme, analysis of all data
flows for plausibility.
The certification program
must at least pretend
must at least pretend that the certification
·
that the certification
that the certification service providers the technical
that the certification service providers the technical and organizational dimensions
that the certification service providers the technical and organizational dimensions checked to the effect that
that the certification service providers the technical and organizational dimensions checked to the effect that that the requirements for
that the certification service providers the technical and organizational dimensions checked to the effect that that the requirements for Ensuring transparency
that the certification service providers the technical and organizational dimensions checked to the effect that that the requirements for Ensuring transparency be complied with
that the certification service providers the technical and organizational dimensions checked to the effect that that the requirements for Ensuring transparency be complied with (document check,
that the certification service providers the technical and organizational dimensions checked to the effect that that the requirements for Ensuring transparency be complied with (document check, methodical analysis).

that the certification
service providers the technical
and organizational dimensions
checked to the effect that
that the requirements for
Ensuring the purpose
binding are adhered to
(document check,
methodical analysis).
Article 5 paragraph 1 letter c
data minimization
The certification criteria must
sen on the to be led
Evidence extend that the
Processing activity in a
economical way
will lead.
The criteria must
tion of this proof in relation
on the fulfillment of the following legal
stipulations:
Fulfillment of the Conditions
according to Art. 5 Para. 1 lit. c:
a) Criteria to determine the appropriate
senheit, the importance and
the need for processing

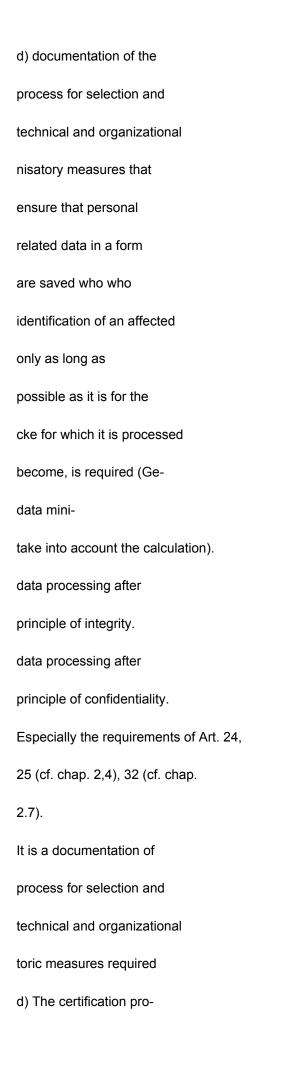
processing of personal
to assess data
b) documentation of the
zesses to ensure
that the processing of personal
personal data of any
time appropriate for the purpose
and significantly as well as on that
necessary amount limited
is. (Warranty target Da-
consider minimizing
gene.)
Article 5 paragraph 1 letter d
accuracy
accuracy  The certification criteria must
•
The certification criteria must
The certification criteria must on the through the Ver-
The certification criteria must on the through the Verresponsible
The certification criteria must on the through the Verresponsible  The certification program
The certification criteria must on the through the Verresponsible  The certification program must specify at least:
The certification criteria must on the through the Verresponsible  The certification program must specify at least:  Document review, legal
The certification criteria must on the through the Verresponsible The certification program must specify at least: Document review, legal cal analysis of the documents
The certification criteria must on the through the Verresponsible  The certification program must specify at least:  Document review, legal cal analysis of the documents and documentation acc.
The certification criteria must on the through the Ver- responsible The certification program must specify at least: Document review, legal cal analysis of the documents and documentation acc. column 2
The certification criteria must on the through the Ver- responsible The certification program must specify at least: Document review, legal cal analysis of the documents and documentation acc. column 2 The certification program

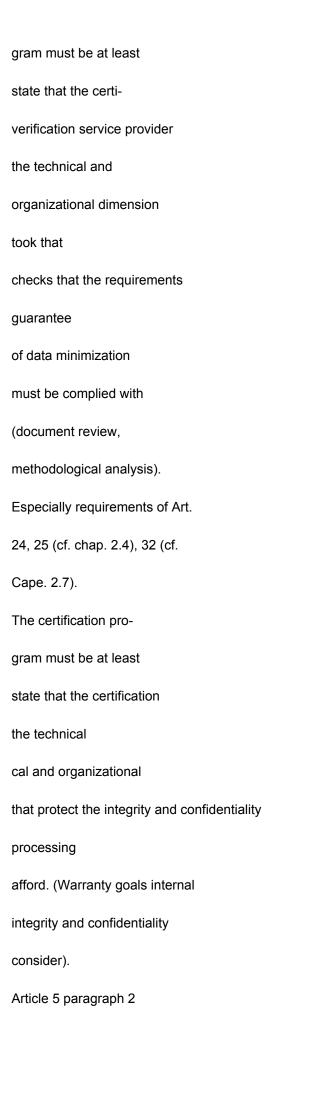


The criteria must
tion of this proof in relation
on the fulfillment of the following legal
stipulations:
Fulfillment of the Conditions
in accordance with Article 5 Paragraph 1 Letter d:
a) Criteria for determining the
factual correctness
personal data,
b) documentation of the
zesses to determine the
factual correctness
personal data,
c) documentation of the
process for selection and
setting suitable technical
shear and organizational
measures that guarantee
that incorrect data
immediately deleted or
correct (guarantee
goal integrity and
i. In conjunction with Art. 16 Intervenable
take into account).
The certification criteria must
on the through the Ver-

responsible
point out that he
work after
Principle of memory limitation
performed.
The criteria must
tion of this proof in relation
on the fulfillment of the conditions
according to Art. Art. 5 Para. 1 lit. e
hen:
The certification program
must specify at least:
Document review, legal
cal analysis of the documents
and documentation acc.
column 2
The certification program
must at least pretend
that the certification
service providers the technical
and organizational dimensions
checked to the effect that
that the requirements for
Ensuring the integrity
ity are complied with
(document check,

methodical analysis).
The certification program
must specify at least:
Document review, legal
cal analysis of the documents
and documentation acc.
column 2
Article 5 paragraph 1 letter f
integrity and confidentiality
a) Criteria for determining the
identifiability of a person
son
b) Criteria for determining the
for the purpose of processing
tion required duration of
identifiability of a person
son
c) Criteria for determining the
suitable form of storage
security of personal
Data identifying
one data subject only
as long as it allows for
the purposes for which they
are required
is,





Proof of compliance with Art.
5 para. 1 (see above).
measures to that effect
checks that the requirements
genes to ensure the
integrity and confidentiality
be respected
(document check,
methodical analysis).
2.3 Article 6: Lawfulness of processing
Processing of personal data is only permitted if there is a legal basis for this
consists. Art. 6 is the central provision of the GDPR on the admissibility of the processing of personal
general data.
Statutory facts
times
Article 6 paragraph 1 (in principle)
Processing is just below
the vo-
suspensions lawful.
In the certification criteria too
audit topics to be dealt with and
ren implementation by the customers
the certification body
a) Presentation, examination and documentation
documentation of a legal

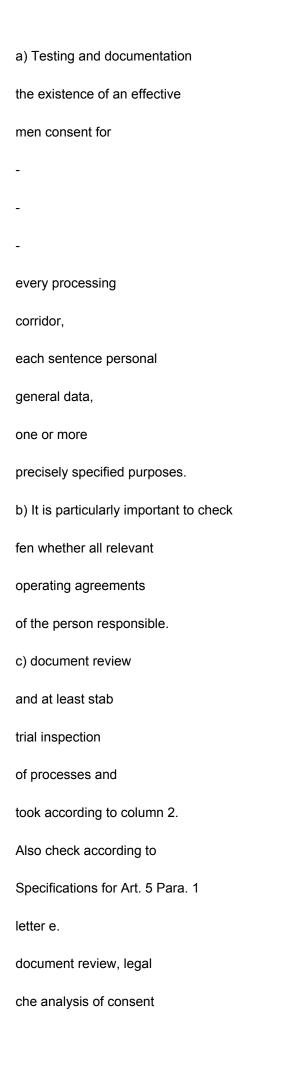
accountability

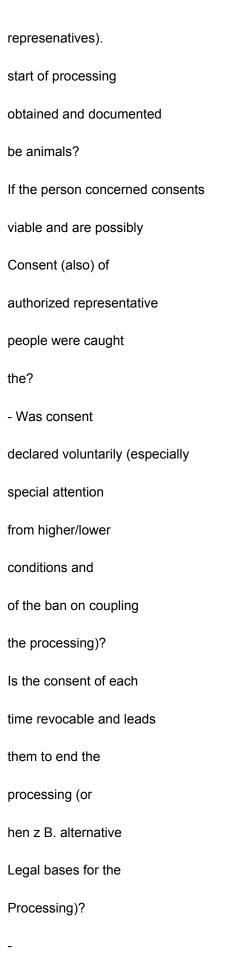
basis for the respective
processing of all personal
related data for each
individual definable
work process; processing
processes that are based on
legal basis
hen, can in the representation
development, testing and documentation
station are summarized
the.
b) Insofar as customers are responsible
cher i.S.d. Art. 4 No. 7 are:
- Documentation of
instructions to the employees
to the upstream
How does the certification
put the implementation?
a) document check,
legal analysis of
presence of one
Legal basis in particular
based on the following
required documents: the
Data protection,
the information acc.

Art. 13, 14, of the of the processing activities acc. Art. 30, of the internal notice, from which the examination and the due to a legal basis location results. b) document review, legal analysis of documentation according to Column 2, e.g. e.g of internal guidelines, service instructions or Article 6 paragraph 1 letter a The person concerned has their consent to the processing processing of those concerned personal data for one or more given proper purposes. Existence check one of legal position, even before a change change/expansion of certification subject

status done; the instruction should sing that too "like" the exam, e.g. Am form of guidelines, write and hints to the examination procedures at the person responsible contain. - Documentation of structural structures and responsibilities for examining a sufficient legal basis location (e.g. if necessary binding of the legal or of the data protection area or other responsible person Place). tation of processes and

c) Existence and documentation tation of processes and took that after the omission of lawfulness of the processing tion to a deletion of the carry data. In particular are also the requirements from Art. 5 Para. 1 lit. e to regard.





- Was the affected person

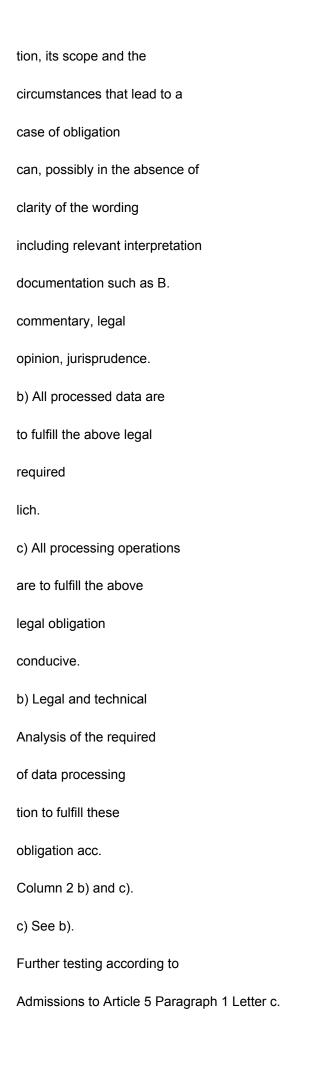
son and, if necessary, the representative
authorized person(s)
son(s) before the declaration
consent sufficient
appropriate and in compliance
of the transparency principle
cleared up?
Designation, examination and documentation
mentation of the existence of the following
requirements:
For events that have already taken place
processing operations
samples of existing
ourified or existing
the consents.
· ·
the consents.
the consents.  document review, legal
the consents.  document review, legal  analysis of the design
the consents.  document review, legal  analysis of the design  the revocation process
the consents.  document review, legal  analysis of the design  the revocation process  as well as inspection. To do this
the consents.  document review, legal  analysis of the design  the revocation process  as well as inspection. To do this  len also the exam and the
the consents.  document review, legal  analysis of the design  the revocation process  as well as inspection. To do this  len also the exam and the  Inspection of the processes that
the consents.  document review, legal  analysis of the design  the revocation process  as well as inspection. To do this  len also the exam and the  Inspection of the processes that  cause the data
the consents.  document review, legal  analysis of the design  the revocation process  as well as inspection. To do this  len also the exam and the  Inspection of the processes that  cause the data  after receipt of an objection
the consents.  document review, legal  analysis of the design  the revocation process  as well as inspection. To do this  len also the exam and the  Inspection of the processes that  cause the data  after receipt of an objection  to be deleted.

ment of the ability to consent ability, especially age verification tion, and (2) the further Procedures in the event of of the failure to consent ability. a) Existence of a contract with the data subject or a) document check, legal analysis Execution of pre-contractual certain measures required ly, which at the request of the affected person takes place. of a pre-contractual container upon request affected person. in particular their are these (contractual) to delimit relationships from the cases of a non-binding of different public offers (e.g. visiting a website) post-contractual relationship and obviously ineffective same contracts.

hand of documentary
tion (particularly
wearing pattern, descriptive
exercises or notes
to pre-contractual
conditions) of the best
hens of a contract o-
that of a pre-
chen relationship with
the person concerned.
b) all processed data are
to fulfill the contract or to
Execution of the pre-
measures required
lich.
c) all processing operations
are to fulfill the contract or
to carry out the
contractual measures
conducive.
d) documentation of structural
and processes that lead to
a contract or
a pre-contractual relationship
not lead.
to b) to d) are in particular

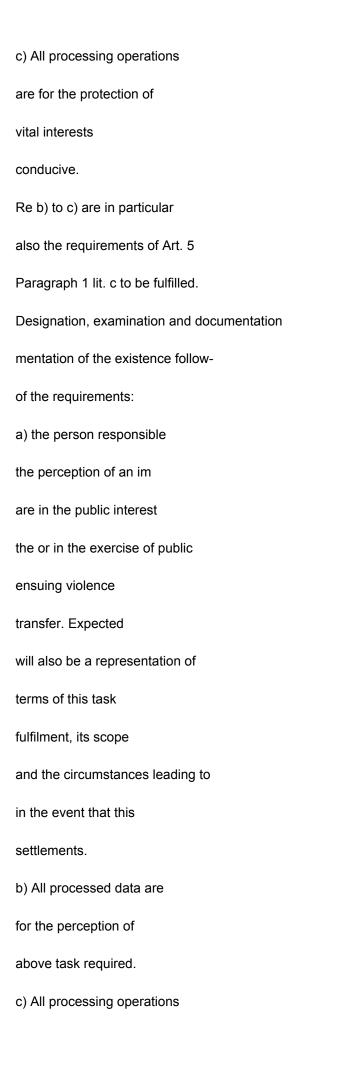
also the requirements of Art. 5
Paragraph 1 lit. c to be fulfilled.
Article 6 paragraph 1 letter c
The processing is to fulfill
ment of a legal
obligation required, the
Designation, examination and documentation
mentation of the existence of the following
requirements:
b) Legal and technical
Analysis of the required
according to Column 2 b) and
c). Furthermore examination
according to the requirements of Art. 5
Paragraph 1 lit. c.
c) See b).
d) Document check of
structures and processes
according to column 2 d) and
inspection of processes,
to a contractual
end or to one
pre-contractual relationship
not lead.
For events that have already taken place
processing operations

at least randomly
term document check
of concluded contracts
gene or received
pre-contractual relationship
senior
the person responsible under
lies.
Article 6 paragraph 1 letter d
The processing is necessary
to protect vital
of the persons concerned
son or another natural
to protect any person.
a) Existence of a legal
a) document check,
Analysis of presence
a legal
responsibility
literal based on the
documentation according to
Column 2 a).
obligation of the responsible
lichen, including one
Presentation of the conditions
the occurrence of this obligation



to b) to c) are also in particular
the requirements of Art. 5 para.
1 lit. c to be fulfilled.
d) The provisions in paragraphs 2 and 3 are included
related regulations
or possibly
pending special regulations
observe.
Designation, examination and documentation
mentation of the following
settlements:
a) Presence of vital
interests of the persons concerned
son or another natural
person. is expected
in particular a
documentation,
and which vital
gen interests are affected.
d) document check,
legal analysis for
observance of the regulations
according to column 2 d).
a) document check,
legal analysis of
presence of vital

interests of a
natural person based
the documentation
according to column 2.
Article 6 paragraph 1 letter e
The processing is for the
performance of a task
required in public
chen interest lies or in
exercise of public authority
takes place, which the responsible
has been transferred.
b) Legal and technical
Analysis of the required
of data processing
tion to protect the above
vital interest
s according to column 2 b) and
c). Furthermore examination
according to the requirements of Art. 5
Paragraph 1 lit. c.
c) See b).
b) All processed data are
for the protection of
important interests require
lich.



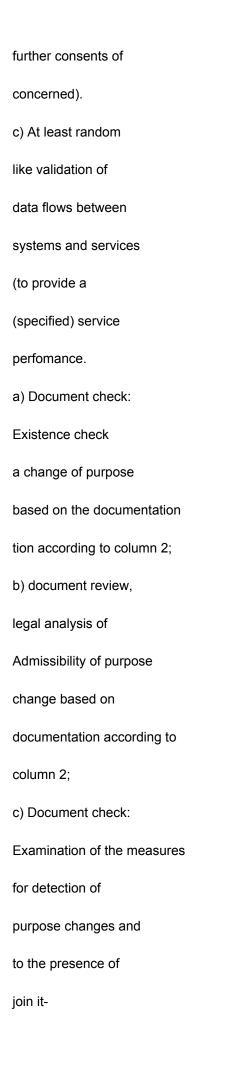
are for perception
the above task required.
a) document check,
legal analysis of
presence of one to the
Responsible over
carried task in
within the meaning of Art. 6 Para. 1
lit. e based on the documentation
ment according to column
2.
b) Legal and technical
Analysis of the required
of data processing
direction to perception
this task acc.
Column 2 b) and c). Further
Test according to
5 (1) lit. c.
c) See b).
Article 6 paragraph 1 letter f
The processing is
legitimate interest
responsibility of the person responsible
or a third party
ly, unless the interest

sen or fundamental rights and
fundamental freedoms of the
NEN person who the protection
personal data
demand, outweigh, especially
especially when it is
at the person concerned
is about a child.
Re b) to c) are in particular
also the requirements of Art. 5
Paragraph 1 lit. c to be fulfilled.
d) In particular, the
Specifications of Art. 6 Para. 2
and 3 as well as possibly
special regulations
e.g. depending on the
context of use, to note
ten.
a) Presentation, examination and documentation
documentation, to what extent
- the processing in the
legitimate interest of
person responsible or
a third party lies
it is not about
hear in fulfillment of their

tasks made
processing,
-
- the interests or
fundamental rights and fundamental
freedoms of those concerned
person do not predominate
especially when
it is a child
acts.
b) documentation of the process
for balancing of interests
specific criteria for the
weighing and corresponding
provides results. the pro
zess must in particular the
Provide representation which
and whose specific interests
sen against which and whose
specific interests or
rights with regard to
which personal
data and which processing
processes are weighed
become.
d) document check,

legal analysis for
observance of the regulations
according to column 2 d).
a) document check,
legal analysis of
existence of advance
stipulations of Art. 6 para.
1 lit. f. based on the documentation
ment according to column
2. It is particularly important to check
dere whether the consideration
correct in each case
was taken. Included
should also random
like records under
be sought, whether this
children are affected o-
who can be and this
in the consideration
appropriately considered
became.
b) testing and inspection
of the process of
food consideration.
Article 6 paragraph 4
In the event of subsequent changes

tion of the processing in order to exist special Requirements according to Article 6 Paragraph 4 if for the new No legal purpose basis exists or the Affected not also with regard to for this purpose a (actual same) consent given have. a) Documentation of the purpose change (of what purpose to which?). b) Documentation of the justification of the change of purpose such as documentation of legal general examination of admissibility the change of purpose. c) Existence of documented measures so that pending changes of purpose be known and the stated purpose in good time checked and, if necessary, further can be made ning (such as obtaining



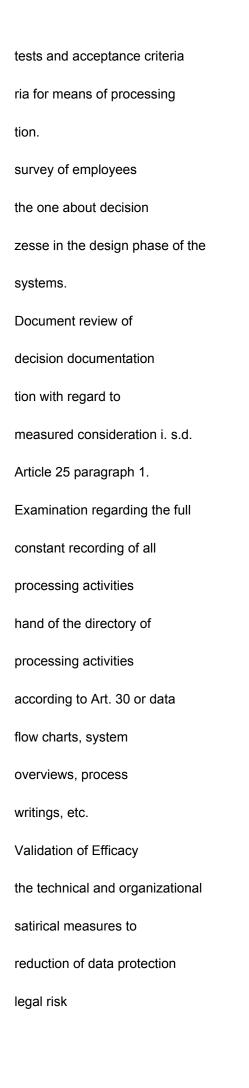
the necessary
turns based on the
documentation according to
column 2 and at least
tens random
inspection of this
measures and precautions
gene.
2.4 Article 25: Data protection by design and by data protection-friendly
che presets
Statutory facts
times
Article 25 paragraph 1
Data protection through technology
layout
In the certification criteria too
audit topics to be dealt with and
ren implementation by the customers
the certification body
There must be a data protection
chemical risk assessment (see also
"Data protection risk
consideration") of the processing
completed and documented
be animal.
It must be state of the art

cares and for the employed Means for processing be taken into account. The means of processing must this stand appropriate follow. (Wei-Other considerations are imcomplementation costs, type of Scope, Circumstances and Purposes of processing, probability of probabilities and severity of associated with the processing risks for the rights and freedoms of natural persons. How does the certification put the implementation? Document check of the safety consideration. survey of employees, which measures to monitoring the status of technology to be taken and whether proposals for allocation of funds measure are taken into account the (see insofar supplementary zend specifications for the "time

point of processing").
Document check of
job descriptions or
work instructions
There must be a description of all
technical and organizational
cal measures to safeguard
the data protection principles and
Admission of necessary guarantee
tien
- to meet the requirements of
GDPR to comply and
- the rights of those affected
to protect people
consist.
Document check of
measures taken
view and validation of
effectiveness of the technical
and organizational dimensions
took to reduce the
data protection risk
kos.
Article 25 paragraph 1
At the time of determination
of funds for processing

suitable technical niche and organizational Measures taken that are designed to data protection principles effective implement and the necessary guarantees in the processing to record the requirements of this to comply with regulation and the rights of those affected to protect people. Article 25 paragraph 1 At the time of processing suitable technical niche and organizational Measures taken that are designed to data protection principles effective implement and the necessary guarantees in the processing to record the requirements of this to comply with regulation and the rights of those affected to protect people.

There must be processes
which the consideration of
Data Protection Principles at the time
point of determining funds
guarantee.
The determination or the
decision for suitable technical
cal and/or organizational
Measures must be documented
and justified (cf. Art. 5
Paragraph 1 lit. f i. in conjunction with Art. 5 Para. 2).
All processing activities must
facts recorded and based
suitable for the risk assessment
technical and organizational
Measures to reduce the
identified risk implemented
(cf. Art. 32 Para. 1).
The determination or the
decision for suitable technical
cal and/or organizational
Measures must be documented
Document review of
process documentation.
Document review from
exemplary tender

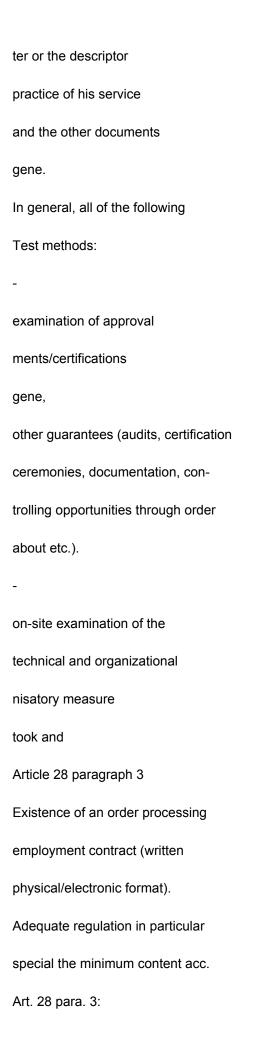


Dogument review of
Document review of
decision documentation
Article 25 paragraph 2
Privacy-friendly pro-
ideas
and justified (cf. Art. 5
Paragraph 1 lit. f i. in conjunction with Art. 5 Para. 2).
All settings of the
Means of processing checked
whether this processing
to the necessary extent
restrict and default to
this limited attitude
and mined database
be set.
be set.
be set.  It must be the necessary amount
be set.  It must be the necessary amount the data collected, the scope
be set.  It must be the necessary amount the data collected, the scope of processing, their storage
be set.  It must be the necessary amount the data collected, the scope of processing, their storage deadline and its accessibility docu-
be set.  It must be the necessary amount the data collected, the scope of processing, their storage deadline and its accessibility docu- be mentioned and justified
be set.  It must be the necessary amount  the data collected, the scope  of processing, their storage  deadline and its accessibility docu- be mentioned and justified  (cf. Art. 5 para. 1 lit. c, e in conjunction with
be set.  It must be the necessary amount the data collected, the scope of processing, their storage deadline and its accessibility docu- be mentioned and justified (cf. Art. 5 para. 1 lit. c, e in conjunction with Art. 5 para. 2).
be set.  It must be the necessary amount the data collected, the scope of processing, their storage deadline and its accessibility docu- be mentioned and justified (cf. Art. 5 para. 1 lit. c, e in conjunction with Art. 5 para. 2).  It must be ensured that
be set.  It must be the necessary amount  the data collected, the scope  of processing, their storage  deadline and its accessibility docu-  be mentioned and justified  (cf. Art. 5 para. 1 lit. c, e in conjunction with  Art. 5 para. 2).  It must be ensured that  personal data not

become.
tion with regard to
measured consideration i. s.d.
Article 25 paragraph 1.
Checking the settings
ner standard configuration
the means of processing,
where all non-required
chen processing operations
must be disabled.
Verification of Necessity
from non-restrictive
Presets based on
processing purposes.
Examination of the documented
restrictions on whether
led reasons of a
ongoing data minimization
resist.
Determination of processing
processes which per-
sun-related data
an indefinite number of
natural persons to
make accessible and
closing document

examination of the specified	
presets.	
2.5 Article 28: Processors	
2.5.1 Introductory Notes	
There are two different perspectives for the test criteria on this point:	
The order processing service should be certified.	
2. The use of a processor by the responsible body should be part of the certification	
be decoration.	
Art. 28 is the central provision for processors in the GDPR. The person responsible may	
According to Art. 28 Para. 1, we only use processors who offer sufficient guarantees	
that they take appropriate technical and organizational measures to ensure adequate data protection	
use. Approved rules of conduct of the	
Processors according to Art. 40 or certifications according to Art. 42 can be used.	
2.5.2 Tabular overview: requirements, forms of implementation and testing	
Statutory facts	
times	
Order processing must be in	
specific use	
and be legal.	
Article 28 paragraph 1	
Sufficient guarantees for	
suitable technical and organizational	
satirical measures.	
In the certification criteria to	
acting test topics and their	
Implementation by the customers of	

Certification Authority
The person responsible must
known information on the part of
processor to his
service to assess
to be able to determine whether the
work in his area
is signed
It must be checked and documented
ren whether an order processing
or a joint responsibility
tion i. s.d. Art. 26 or exists.
Depending on the application, the
specifics of admissibility or
any existing restrictions
to be observed (e.g. with regard to processing
Management of personnel files on behalf
or in the health sector).
Existence of approved behavior
regulate (Art. 40) or
Certification (Art. 42) or
How does the certification
the implementation
tongue?
Examination of the offer text
of the order processor



- Subject and duration of the
- Document review.
- Legal analysis of the
contract in full
security and legal
Admissibility.
Incoming legal
examining the concrete
contractual implementation
and the curtain
denseins sufficient-
the technical and
organizational
Measures (cf
Measures (cf Statements on Art.
·
Statements on Art.
Statements on Art. 32).
Statements on Art. 32).
Statements on Art. 32). work (Art. 28 para. 3 sentence 1);
Statements on Art.  32).  work (Art. 28 para. 3 sentence 1);  -  - Type and purpose of processing
Statements on Art.  32).  work (Art. 28 para. 3 sentence 1);  -  - Type and purpose of processing  (Art. 28 para. 3 sentence 1);
Statements on Art.  32).  work (Art. 28 para. 3 sentence 1);  -  - Type and purpose of processing  (Art. 28 para. 3 sentence 1);
Statements on Art.  32).  work (Art. 28 para. 3 sentence 1);  -  - Type and purpose of processing  (Art. 28 para. 3 sentence 1);  - Type of personal  -
Statements on Art.  32).  work (Art. 28 para. 3 sentence 1);  -  - Type and purpose of processing  (Art. 28 para. 3 sentence 1);  - Type of personal  -  data (Art. 28 para. 3 sentence 1);

for the contractor (Art. 28 para. 3 lit. a); - guarantee of trust confidentiality or secrecy (Art. 28 para. 3 lit. b); taking adequate technical shear and organizational Order processing measures beiters (Art. 28 Para. 3 lit. c); - Rules for claiming of subcontractors (Art. 28 Paragraph 3 lit. d); - Order support contractor in his duty to Responding to requests on perception of meeting rights. are for this suitable at the contractor technical and organizational cal measures guaranteed (Art. 28 para. 3 lit. e)? - Support requirements of the person responsible at the compliance with the specifications Art. 32 to 36 (Art. 28 para. 3 lit.

f);
- Specifications for deletion/return
after completion of the
agreed service (Art. 28 para.
3 letter g);
Article 28 paragraph 4
contract with additional
subcontractor
participant (written/electronic
cal format).
Article 28 paragraph 2
Subcontractors only with
written approval.
Article 44
Existence of appropriate guarantees
when data is transmitted to a
third country.
Article 33 paragraph 2
Ensuring an immediate
general reporting of data
breaches of protection as soon as these
-
-
Provision of all
required information
by contractor to the

```
responsible for
of the obligations (Art. 28 para.
3 lit. h, Art. 5 Para. 2);
enabling verification
gene (including inspection
) (Art. 28 Para. 3 lit. h) or
presence of a process
the person in charge, with
which this compliance with
Specifications from the contractor
can continuously monitor;
- Agreement of an information
Obligation of the order processing
if he thinks
sung is to be an instruction
unlawful (Art. 28 para. 3 lit.
H).
Drafting a contract i. s.d. Before-
provisions of Art. 28 Para. 4 i. V. m.
paragraph 3.
Sufficient guarantees regarding technical
nical and organizational dimension
took
presence of a process of
makes sure when planning
the commissioning of a new company
```

a teaching contractor
of the client or entity
approval is granted.
Documentation of the approval
gene.
Documentation of Guarantees
(cf. Art. 5).
- Legal analysis of the
-
-
-
contract in full
eligibility and admissibility
ability;
Checking the documents
tation of the techn./org.
Measures;
on-site examination of the
tech./org. measures
men.
If already one
(new) subcontract
contractor commissioned
was, checking whether
corresponding sub
directions/approval

ments have been made;
- document verification;
- Audit of the processes.
-
Checking the documents
tation (cf. Art. 5).
setting up appropriate pro-
cess.
Documentation.
- process audit;
- review of the documentation
comment
the processor
can be.
Art. 32 para. 4, Art. 29
Ensuring that processing
only in accordance with instructions
he follows.
presence of appropriate
processes and documentation
instructions
-
Checking the documents
station
- Description of the
cess.

2.6 Article 30: Record of processing activities

must have already taken place for this.

2.6.1 Introductory Notes

The examination of the criteria of Art. 30 is largely based on the feature of the completeness of the Directory of processing activities. The directory forms a set of (partial) results results from other processes, which are considered under separate test criteria. That's how she can Determination of the processing purposes (Art. 30 Para. 1 lit. b) or the technical-organizational measures (Art. 30 para. 1 lit. g) not only take place within the framework of the maintenance of this register, but

When examining the directory itself, processes within the organizational sation of the person responsible, which contribute to the fact that the directory as a "living" document constantly and truthfully reflects the actual status of the processing activities.

The special situation of small and micro-enterprises is taken into account by the fact that the

The requirement to keep a record of the processing activities may be omitted and that

is pre-examined (see recital 13).

2.6.2 Tabular overview: requirements, forms of implementation and testing

Statutory facts

times

In the certification criteria to

acting test topics and their

Implementation by the customers of

**Certification Authority** 

How does the certification

the implementation

tongue?

Article 30 paragraph 5

List of processing

activities is required.
Checking the requirements:
- Number of employees and
possibly either
- Risk to freedoms and
survey or documentary
test to determine
number of employees
working.
Rights of Individuals
available,
- not just occasional
beitung, or
- processing special category
categories according to Art. 9 Para. 1 or
Article 10.
Legal and technical
organizational documentation
ment test of a dated
responsible
leading rating
- the risk,
- the frequency and
- of the affected cat-
personal
general data

the processing activity
ten.
Article 30 paragraph 1
Directory is complete.
The directory of processing
activities contains all information
from Art. 30 Para. 1 lit. a-g.
Document review of
directory of processing
work activities.
Processes for updating the
Directories are established for
the case that
Examination fixed in writing
process descriptions;
Audit of the processes.
- processing activities
be led
- Processing activities away-
fall,
refer to already listed
processing activities
according to Art. 30 para.
1 lit. a-g change.
-
There are processes for

There are processes for

ongoing cooperation between
-
to the processing activities
departments involved
gene,
- the representative of the responsible
-
as well as
if necessary, the data protection officer
wore
Corresponding responsibilities in
within the organization are
clears.
Document review from
-
fixed in writing
process description
gene,
- organization charts,
- Business/Task-
-
distribution plans;
if necessary questioning of
responsible.
Article 30 paragraph 2
Directory contains information

The directory of processing
activities contains all information
from Art. 30 Para. 2 lit. a-d.
Document review of
directory of processing
work activities.
Processes for updating the
Directories are established for
the case that
Examination fixed in writing
process descriptions;
Audit of the processes.
Document review from
-
fixed in writing
process description
gene;
- organization charts;
- Business/Task-
-
distribution plans;
f necessary questioning of
responsible.

for processors.

-
Categories of in order
processing
activities are introduced;
Categories of in order
processing
activities are omitted;
refer to already listed
Categories of processing
activities according to
in accordance with Art. 30 Para. 2 lit. a-d än-
other
additional responsible persons, in
whose order a processing
is carried out,
come;
-
- Responsible persons on whose behalf
carry out a processing
is led to fall away;
with existing responsibilities
literal, on their behalf
processing performed
will, information according to Art. 30
Change paragraph 2 letters a-d.

-

There are processes for
ongoing cooperation between
-
to the processing activities
departments involved
gene;
- the representative of the responsible
who, as order processor,
ter occurs;
if necessary, the data protection officer
borne by the person responsible
who act as processor
kicks;
-
- those responsible, in whose
order processing
is carried out.
Corresponding responsibilities in
within the organization are
clears.
Article 30 paragraph 3
directory is made in writing
leads.
Article 30 paragraph 4
Directory is available upon request

made available.
The written management of the
drawing is given.
document review.
Appropriate storage
/locations are those involved
people known.
Processes are established to
Document review from
- the receipt;
- the editing;
- the answer under Zurver-
provision of the directory
of the processing activity
ten
-
fixed in writing
process description
gene; Audit of the
cede
- organization charts;
- Business/Task-
a related request
supervisory authority in a timely manner
place.

distribution plans;

if necessary questioning of

responsible.

The distribution of the appropriate

Responsibilities within the organization

organization is clear.

2.7 Article 32: Security of processing

2.7.1 Introductory Notes

Art. 32 requires the implementation of appropriate technical and organizational measures to protect personal data. For the purpose of reviewing these measures, it is required that all relevant measures and processes are documented and the documentation available for examination. On the other hand, it must be ensured that all relevant measures and proare technically or physically accessible for appropriate testing so that their functional can be evaluated wisely. When defining the technical and organizational measures, the Determining the level of protection is decisive. The latter needs to be documented as well as continuous be checked.

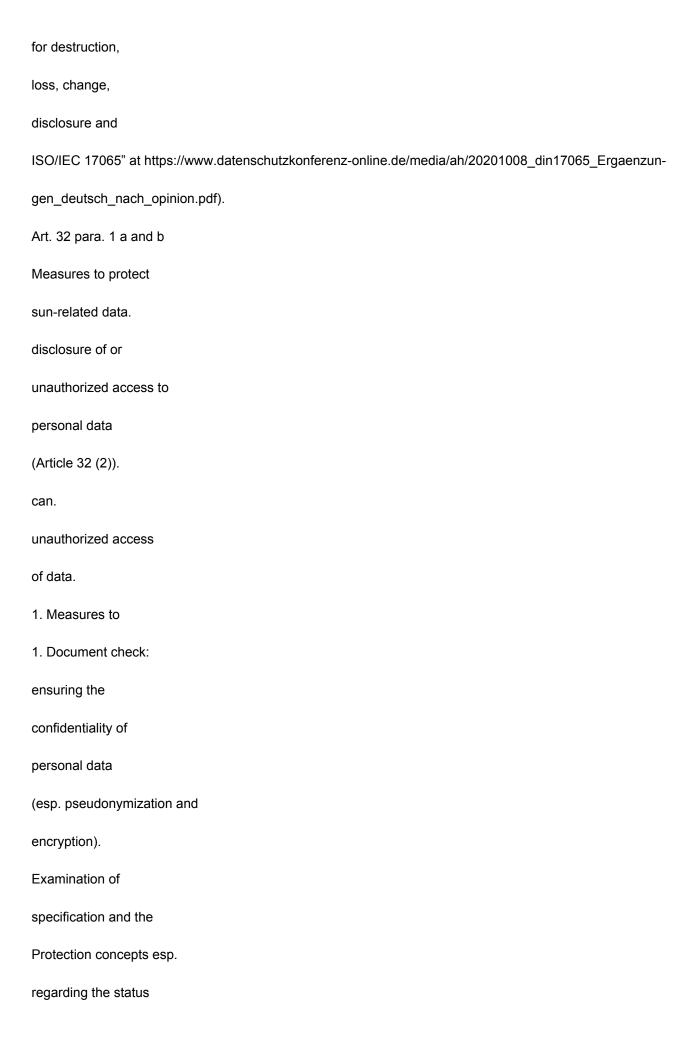
Certain requirements resulting from Art. 32 can already be fully or partially through the existence of suitable (IT security) certifications (such as ISMS according to ISO 27001, BSI basic protection), which also include the subject of data protection certification, be covered, cf. supplementary paper of the DSK.10 The fulfillment of the corresponding data protection 10 However, such certifications are only recognized by accredited certification bodies and according to the provisions in Section 7.4 im

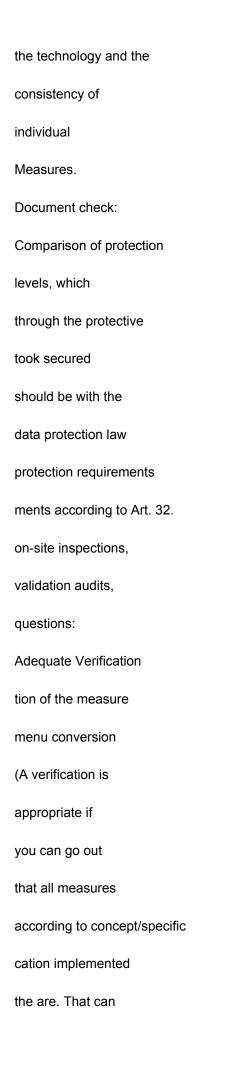
Supplementary paper of the DSK ("Requirements for an accreditation according to Art. 43 in conjunction with DIN EN requirements of one or more (IT security) certification(s) must be fully accuracy and correctness are checked and documented. A data protection requirement is completely and correctly if they clearly meet one or more requirements of an (IT security

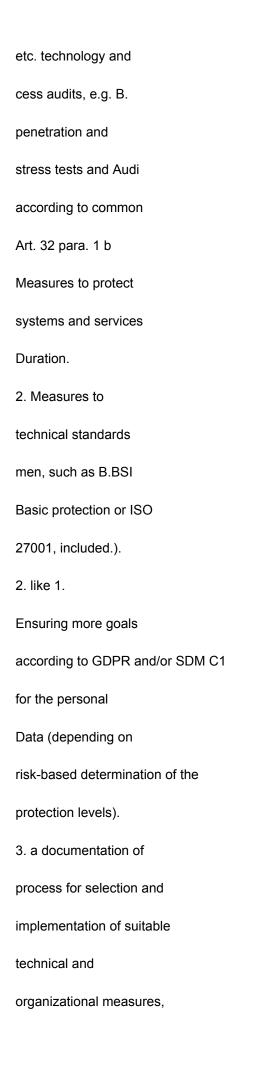
security) certification can be assigned and the test methods used by an (IT security
ness) certification to fulfill the test methods under data protection law are also provided
are equivalent to.
2.7.2 Tabular overview: requirements, forms of implementation and testing
Statutory facts
times
In the certification criteria to
acting test topics and their
Implementation by the customers of
Certification Authority
How does the certification
the implementation
tongue?
Art. 32 para. 1 and para. 2
Defining the level of protection
for all necessary processes
work activities.
1. Complete, detailed
1. document check,
description of all
processed data or
data categories.
2. Risk-based determination of the
adequate levels of protection
(especially taking into account
of recitals 38 and

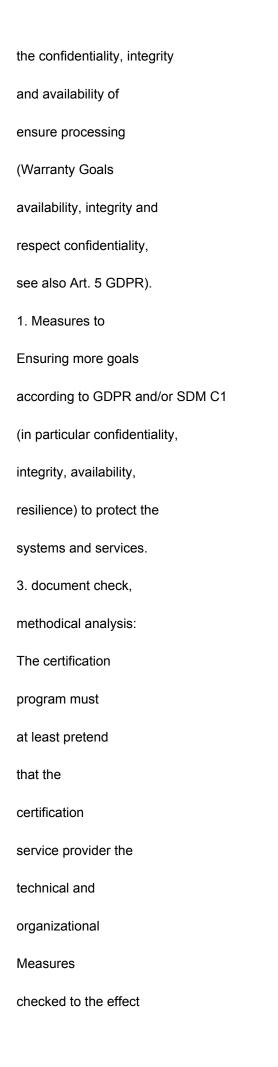
3. consideration of risks,
which stand out in particular
destruction, loss,
change, unauthorized
questioning of
responsible.
2. Examination of
conformity of
used
Risk method with the
GDPR.
Document check:
correctness check
the risk assessment
(e.g. according to SDM D3).
document review,
legal analysis:
Comparison of the result
current protection levels
with the protection requirements
to be processed
data cate-
goria.
3. like 2. with the
focus

75).



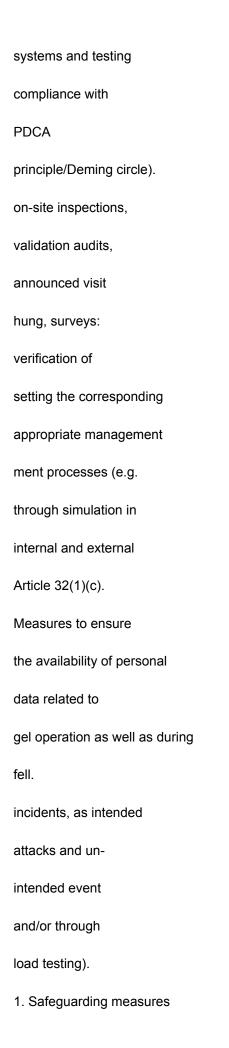






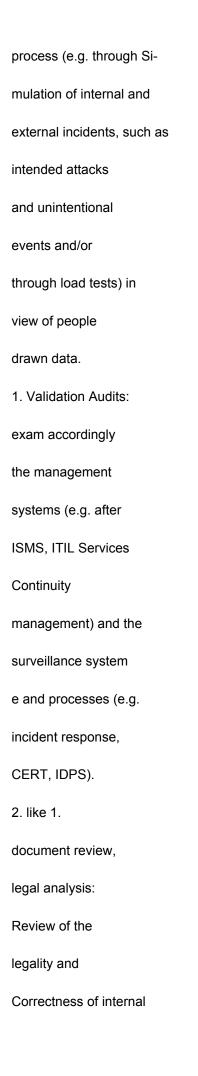
that the
requirements for
ensuring the
Availability,
integrity and
confidentiality
be respected.
1. Document check:
Examination of
specification and the
Protection concepts esp.
regarding the status
the technology and the
consistency of
individual
measures (esp.
authorization concept,
identity mana
mind,
authentication and
authorization,
revision and
2. Guarantee of
Measures (from point 1) on
Duration.
logging

concept).
The level of protection
measures must den
protection requirements
to the overall system
match (e.g.
according to IT security
concept). examination
follows by a
even.
on-site inspections,
validation audits,
questions:
Adequate Verification
tion of the measure
menu conversion (see
above).
2. document check,
Surveys:
audit of the operating
continuity concept,
e.g. B. according to BSI 200-4
or ITIL
(especially exam
the completeness of
coverage more relevant



1. Document check:
the availability
personal data in
regular operation.
2. Guarantee of
Availability at physical
or technical
incidents.
Examination of
specification and the
relevant concepts
(e.g. verification of
availability classes,
service level
agreements) esp.
regarding the status
of the technique.
That through the
took guaranteed
availability level
must have the
ability requirements
the processed personal
sun-related data
correspond to
speaking of risk
opeaning or new

based determination
according to Art. 32 Para. 1).
Exam done by
a comparison.
on-site inspections,
validation audits,
questions:
Adequate Verification
tion of the measure
menu conversion (e.g.
according to ITIL Availability
Management, KRITIS).
2. Document check:
Examination of
Availability and
recovery
concepts (e.g. after
ISO 2700x).
on-site inspections,
validation audits,
announced visit
hung, surveys:
verification of the in
above mentioned
included
measures and

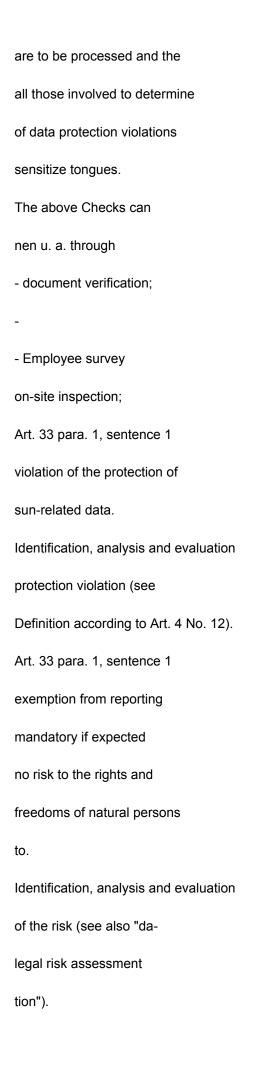


guidelines and agreement Article 32 paragraph 1 letter d Measures to guarantee of regular overtesting, evaluation and luating the effectiveness of the technical and organizational measures. Art. 32 para. 4 Measures to ensure ment that the responsible or the order processing subordinate natural persons these personal gene data only 1. Ensuring that all relevant systems and processes of a regular review, evaluation and Evaluation with regard to effectiveness of the TO subject to action. 2. Guarantee that the under 1. established measures

all systems and processes

implemented correctly (effectively).
are.
ensuring that
Processing Agreements
personal data
exist and are correct.
on appropriate instructions
process.
document check,
questions:
Check whether the above
called guidelines and
agreements of the
nisatory structure of
responsible according to
chen.
2.8 Articles 33 and 34: Reporting personal data breaches
Data to the supervisory authority and notification of a breach
affected person
2.8.1 Introductory Notes
Art. 33 and Art. 34 regulate the reporting to the supervisory authority and the notification to the
data subject in the event of a personal data breach.
Specifically, the content and deadline of the report/notification, documentation and manual
obligations as well as possible exceptions to the obligation to report/notify.
2.8.2 Tabular overview: requirements, forms of implementation and testing
Statutory facts

times
Article 33
Obligation to report to supervisory
hear.
In the certification criteria too
audit topics to be dealt with and
ren implementation by the customers
the certification body
There must be a process for
nalization be fixed, as with
to avoid data breaches
drive is to meet the requirements
comply with the reporting obligation.
This includes i.a. the definition
of process steps and
responsibilities, what the
qualification of all those involved
determination of data protection
generally with
takes.
How does the certification
put the implementation?
Check whether and to what extent
wide procedures/pro-
present in the event
a data protection incident



take place.
SO.
so.
Art. 33 para. 1 sentence 1 deadline
("immediately and as far as possible
within 72 hours"),
Measures to meet deadlines
Determination of breaches of deadlines
and, if necessary, justification.
SO.
Art. 33 Para. 1, Sentence 2 Justification
liability in the event of a deadline
tongue.
Article 33 paragraph 2
Reporting obligation of the contract
worker to the responsible
Art. 33 para. 3
content of the message.
Article 33 paragraph 3 letter d
Remedial Actions
of the injury and
if necessary, measures to
mitigating their possible
adverse effects.
measures to ensure

that the processor
breach of protection to the
verbal reports (possibly regulation
in the order processing contract).
Measures to ensure
complete report
dung; possibly use supervisory
official reporting forms.
Selection and implementation of
technical and organizational
measures.
Regarding the measures, please refer to
tification, analysis and evaluation
the protection violation and the risk
to turn off kos (see above).
see above, especially examination of the
contract processing contract.
SO.
SO.
exception regarding the
stop the message:
Article 33 paragraph 4
Gradual availability
information.
Art. 33 para. 5, sentence 1
documentation requirement.

Article 34 obligation to notify affected person. information will be after Art. 33 para. 4 progressively made available. The reporting deadline according to Art. 33 Para. 1, Sentence 1 basically also preserved will if the required Minimum information according to para. 3 not observing the deadline at the same time time available. In this case, the required relevant content/scope of the tion gradually available be asked, which leads to a table "must" of the gradual Provision of the information tion in favor of the deadline tion leads (first and subsequent manure). Measures to meet deadlines and for (gradual) subsequent submission the required information are to be taken.

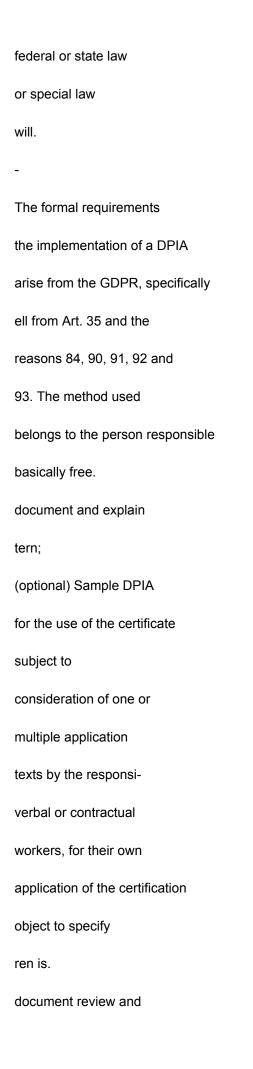
documentation of the violation

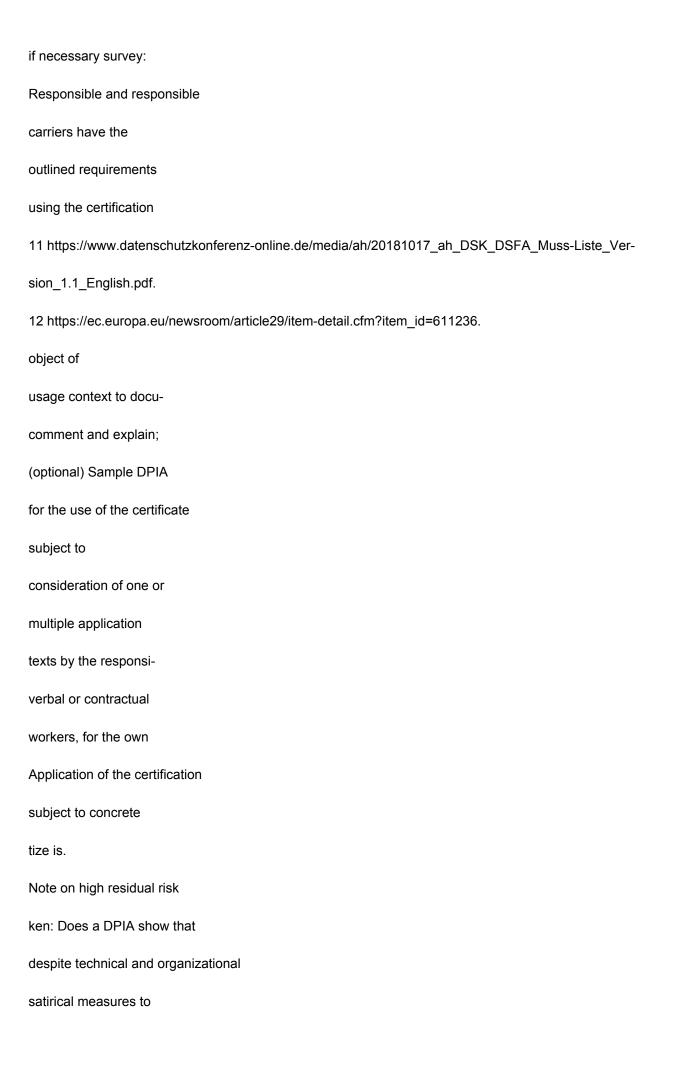
the constantion of a constant data
the protection of personal data
data including all
related to the injury
standing facts, of which
effects and the taken
remedial actions.
The documentation must
permit the supervisory authority
compliance with the provisions of
Article 33 to review.
A procedure must be established
be, as in the case of data protection
action is to be taken
to meet the requirements of
to meet the requirements of so.
·
SO.
so.
so. so. The procedures/pro-
so.  The procedures/prosee Art. 33
so.  The procedures/prosee Art. 33  can be checked.
so.  The procedures/prosee Art. 33  can be checked.  obligation to notify
so.  The procedures/prosee Art. 33  can be checked.  obligation to notify  to meet the affected persons
so.  The procedures/prosee Art. 33 can be checked. obligation to notify to meet the affected persons men. This includes i.a. the festival
so.  The procedures/prosee Art. 33 can be checked. obligation to notify to meet the affected persons men. This includes i.a. the festival tion of process steps and

violation of the protection of
sun-related data with
likely to be at high risk.
Article 34 paragraph 1
deadline
see above on Article 33.
Article 34 paragraph 2
content of the notification
see above on Article 33.
Article 34 paragraph 3
exception to the
obligation to correct
Article 34
documentation of compliance
of the requirements
Check whether exception
stands available.
The documentation must
permit the supervisory authority
compliance with the provisions of
Article 34 to review.
2.9 Article 35: Data Protection Impact Assessment
Statutory facts
times
In the certification criteria too
audit topics to be dealt with and

ren implementation by the customers
the certification body
How does the certification
put the implementation?
Article 35
Necessity test
Obligation to data protection
Impact assessment (DPIA) for a
a potentially high risk
Use of the certification object
stands in the application context
(The determination of the necessary
ness is usually about the
Description of the planned
work processes and the
document review and
if necessary survey:
Responsible and responsible
carriers have the
DPIA-specific examiner
results using the
subject of certification
in the application context
Article 35
minimum requirements
respective processing purposes

```
consequences. Therefore, the decisive factor is
Creation of a directory
of processing activities
according to Art. 30).
For this purpose, it must be checked whether at least
tens by the certification
subject of covered processing
process in one of the following
mentioned in the lists:
special requirements
Article 35 paragraph 3;
- the list according to Art. 35 Para. 4
(white list)11;
- the list according to Art. 35 Para. 5
(Black list).
It is also necessary to check whether the
subject of certification
DPIA for other reasons
is to be supplied, e.g. B. because
- the processing of personal
drawn data requirements
of the EDPB in the current
ellen version (e.g. from
WP248) fulfilled12;
a DPIA due to a
```





risk containment continues
a high risk for the
rights and freedoms of course
more people
(residual risk), according to Art.
36 the person responsible for the
Supervisory authority
consult.
The GDPR does not contain any explicit
formal requirements for
management of the DPIA. In Art. 35 para.
7 but elements are
counts that the impact assessment
must contain at least:
-
-
-
A systematic description
the planned processing
processes and the second
of processing, if
if applicable, including those of
the person responsible
followed legitimate interests
sen
an assessment of the

and proportionate
of processing
gears in relation to the purpose;
an assessment of the risks
for rights and freedoms
of the persons concerned
according to paragraph 1 and
- to cope with the risk
planned remedial measures
guaranties, including
tien, safety precautions
and procedures by which the
Protection of personal
Data secured and the
proof is provided that
that this regulation [also
perspektivisch13] complied with
will, with the rights and
legitimate interests of
affected persons and
other affected legal
is worn.
2.10 Data transfer to third countries or to internal organizations
Does the subject of certification imply a transfer of personal data to third countries
or to international organizations (hereinafter "third country transfer"), the legal requirements are
stipulations regarding the lawfulness of such a third-country transfer from Articles 44 to 49 must be observed.

13 A DPIA is not a one-off process and - based on a changed risk situation or in the event of significant changes - ments in the procedure to be carried out again. In this respect, an iterative process of review and adjustment is recommended len.

This means that a certification program must aim to verify that a third-party
land transfer is part of the subject matter of the certification and is legally permissible.

This results in the following mandatory contents of a certification program, which as a certification

1. Dealing with the question of whether a third-party

tion criteria to be dealt with are:

land transfer can be excluded. The certification authority must note that it in practice, this often leads to such third-country transfers when transferring data within the framework from maintenance, care and support. The relevance of such a transfer is often overhen, especially when maintenance, care and support services are not the focus of the object of certification or the transmission is not provided in the standard case can be seen, but may be necessary in exceptional cases. Therefore, certification bodies and program owner when asked to what extent a transfer to a third country can be ruled out, also keep an eye on such services and do this in a targeted manner as part of the certification program check over.

2. Insofar as a transfer to a third country cannot be ruled out within the scope of the can, customers of the certification body must check and document (and accordingly must be checked by the certification body), on which legal basis the third-country transdone. Within the scope of the so-called 2-stage test, it is to be determined and documented that (1) whether, regardless of specific requirements for the third-country transfer, all other requirements requirements of the transmission in question are complied with and (2) to what extent the specific fishing requirements of Articles 44 to 49 are observed.

With regard to the 2nd stage, in particular the presentation, examination and documentation is expected tation, on what basis of transmission the third country transfer, in particular also the scope,

according to the duration and the purpose.

The following bases of a third-country transfer come into consideration:

- 1. An adequacy decision by the commission within the meaning of Art. 45;
- 2. Appropriate guarantees within the meaning of Art. 46 (possibly in conjunction with Art. 47);
- 3. Exceptions (to be interpreted narrowly) pursuant to Article 49,

in each case taking into account in particular the official practice, the developments in relation to the Determination of the appropriate level of protection and case law (e.g. the "Schrems II" judgment of the ECJ14).

2.11 Rights of data subjects

The following data subject rights are mandatory in a certification program as certification criteria ria to treat:

- 14 Judgment of the European Court of Justice of 16 July 2020 (Case C311/18).
- 1. Transparency and modalities for exercising the rights of the data subject pursuant to Art.

12;

Duty to provide information when personal data is collected in accordance with Articles 13 and 14;

- 2.
- 3. The data subject's right to information pursuant to Article 15;
- 4. Right to rectification according to Article 16;
- 5. Right to erasure ("right to be forgotten") pursuant to Article 17;
- 6. Right to restriction of processing pursuant to Article 18;
- 7. Obligation to notify in connection with the correction or deletion of personal data or the restriction of processing in accordance with Article 19;
- 8. Right to data portability in accordance with Article 20;
- 9. Right to object according to Article 21;
- 10. Automated decisions in individual cases including profiling in accordance with Article 22.

If one of the points listed is not relevant for the certification object under consideration

a justification must be provided as to why this is not the case for the specific subject of certification is required.

3 processes during the validity period of the certification

In order for a certification program to be applied, criteria must be established by the responsible independent supervisory authority to be approved. To do this, the subject of certification must be closing processes are defined and implemented and organizational measures are taken the. As part of the data protection management anchored in the organization, these processes should ensure that the GDPR conformity of the object of certification over the entire period of validity period of data protection certification is maintained. These processes occurs in In connection with a data protection certification, it has a kind of double function.

On the one hand they are part of the organization's own data protection management, on the other hand however, from the point of view of certification, they are also an integral part of the certification stand. As such, they are the subject of data protection checks in the certification process. testing and evaluation by the certification body and thus by the certification granted, however, this only insofar as they relate to the object of certification. A certification of the entire organization's own data protection management does not take place here. Adequate testing and long-term functionality of these processes and thus also a valid and verifiable seal of approval that lasts for the period of validity of the certification. To be able to guarantee this, clearly separate responsibilities and obligations must be define and ensure responsibilities. For this purpose, the tasks of the certification body and the owner of a data protection seal or test mark to be clearly distinguished from each other. They are to be presented in such a way that both the competences and the responsibilities of the respective

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

emerge.

Certification authority as well as the owner of a data protection seal or test mark from it clearly

Data protection specific management processes that govern the CA's relationship with the
Describe the owner of a data protection seal or test mark (including ensuring the
Provision of the contact details of the specific contact persons including their powers
on both sides,),
Processes for permanent compliance with data protection principles according to Article 5;
Data protection-specific processes to protect the rights of data subjects in accordance with Articles 12 to 22;
Processes for risk assessment under data protection law in accordance with Article 30 i. in conjunction with Articles 35 and
36;
Processes for dealing with personal data breaches pursuant to Article 33
and 34
- with identification, analysis, technical evaluation and legal assessment with it-
associated risks of protection violations for the owner of a data protection seal or -
test mark and
- with the selection and implementation as a result taken technical-organizational
Measures according to Article 33 Paragraph 3 Letter d;
Implementation of technical-organizational measures from the process point of view, which may be
supported processes can be controlled and monitored and taking into account and
application of Articles 25 and 32 are to be implemented;
Presentation of the valid, process-supported transformation of data protection requirements

ments in systems and services for which a suitable and appropriate form of technical
to ensure assessment and to provide a possibly recurring legal assessment
ensure is.15
15 Such an assessment of the processes derived from the transformation of the data protection requirements is
certification program as well. A possible guide to carrying out such a transformation is
the standard data protection model (see also https://www.datenschutz-mv.de/datenschutz/datenschutzmodell/).
4 List of Abbreviations/Glossary
TFEU
Treaty on the Functioning of the European Union
AkkStelleG
Accreditation Body Act
kind
BDSG
BSI
CERT
Article
Federal Data Protection Act
Federal Office for Security in Information Technology
Computer Emergency Response Team
DAkkS
German Accreditation Body GmbH
DPIA
DSK
Data protection impact assessment (Article 35 GDPR)
Data Protection Conference
GDPR

General Data Protection Regulation
EDSA
acc.
IDPS
ISMS
ITIL
European Data Protection Board
according to
Intrusion Detection Prevention Systems
Information security management system
Information Technology Infrastructure Library
CRITIS
Critical Infrastructures
PDCA cycle
Plan-Do-Check-Act, Deming circle
SDM
Standard Privacy Model
For the glossary, Annex 1 of the DSK supplementary paper on "Requirements for accreditation
according to Art. 43 Para. 3 DS-GVO i. in conjunction with DIN EN ISO/IEC 17065".