European Privacy Seal

– privacy at its best

EuroPriSe Criteria

for the certification of processing operations by processors (scope: DE)

v3.0

EuroPriSe Criteria

Processing operations by processors

(v3.0 – Date of publication: 15.11.2022)

EuroPriSe Cert GmbH

Joseph-Schumpeter-Allee 25 - D-53227 Bonn

Table of contents

1. Requirements from a legal perspective

This chapter is structured as follows:

- General requirements for processors,
- Requirements with regard to Art. 28 GDPR (relationship processor - controller),
- Requirements with regard to Art. 28 GDPR (relationship processor - other processor),
- Requirements relating to specific types of processing operations; and
- Data protection by design and by default.

1.1. General requirements for processors

1.1.1. Record of processing activities

Requirement in a nutshell:

The processor SHALL in any case maintain a record of processing activities pursuant to Art. 30 par. 2 GDPR, regardless of the exemption provision of Art. 30 par. 5 GDPR. It SHALL also have processes in place to continuously update the record.

Requirement in detail:

Conditions for / exceptions to the applicability of the requirement:

This requirement shall always be applicable, regardless of the exemption provision of Art. 30 par. 5 GDPR.

Details on the subject of the requirement:

The following individual requirements must be met:

1. The record of processing activities relating to the processing operations to be certified SHALL be kept in writing, which may also be in an electronic format.

2. The record SHALL contain the name and contact details of the processor and, if applicable, its representative (cf. Art. 27 GDPR) and/or any data protection officer (Art. 37 ff. GDPR). In this respect, information on postal, telephone and electronic accessibility SHALL be provided.

3. The record SHALL contain the name and contact details of each controller on behalf of which the processor is acting and, if applicable, its representative (cf. Art. 27 GDPR) and/or any data protection officer (Art. 37 ff. GDPR).[1] In this respect, information on postal, telephone and electronic accessibility SHALL also be provided in each case.

4. The record SHALL contain the categories of processing operations that are within the scope of the EuroPriSe certification.[2]

[1] Where the certification customer acts as a sub-processor (if at all), it only has to name his direct principals, but not the further chain behind them back to the controllers.

[2] Other processing activities which the certification customer may also carry out on behalf of the controllers are irrelevant for the specific certification procedure and can therefore be omitted or blacked out in the record.

5. The record SHALL contain, where applicable, information on transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation. Where data are transferred to a third country, the specific recipients of the data in the third country SHALL also be indicated. If the transfers are made on the basis of Art. 49 par. 1 subpar. 2 GDPR, the documentation of the suitable safeguards provided for SHALL also be listed.

6. The record SHALL contain a general description of the technical and organisational security measures (TOM) referred to in Art. 32 par. 1 GDPR that have been implemented with regard to the processing operations to be certified. In this respect, the specific reference to a separate document describing the TOM is sufficient.

7. The processor SHALL have processes in place to continuously update the record in the event that

- categories of processing activities processed on behalf of the controller are introduced resp. cease to exist,
- additional controllers on whose behalf processing is carried out are added resp. cease to exist,
- information pursuant to Art. 30 par. 2 lit. a)-d) GDPR changes for categories of processing activities already listed and/or existing controllers on whose behalf processing is carried out.

8. The processor SHALL have processes in place that govern the cooperation of the relevant actors with regard to the updating (cf. No. 7 above) of the record (in this respect, the following shall be mentioned: specialised departments of the processor involved in the processing activities to be certified, the representative and/or the data protection officer of the processor, if applicable, and controllers on whose behalf the processing operations are carried out).

Relevant national law (if applicable):

N/A

1.1.2. Designation of a data protection officer

Requirement in a nutshell:

The processor SHALL have designated a data protection officer and documented this if it has an obligation to do so under Art. 37 GDPR or under any applicable national law. In that case, the processor SHALL also meet the requirements for the professional qualities of the DPO as well as the organisational requirements listed below at “Requirement in detail”.

Requirement in detail:

Conditions for / exceptions to the applicability of the requirement:

The processor SHALL designate a data protection officer if at least one of the following statements applies:

1. The processor is a public authority or body as determined by national law, except for courts acting in their judicial capacity.

2. The core activities[3] of the processor consist of processing operations which, require regular and systematic monitoring of data subjects on a large scale.

   Monitoring is “regular” if one or more of the following factors are present:

   - Ongoing or occurring at particular intervals for a particular period;
   - Recurring or repeated at fixed times;
   - Constantly or periodically taking place.

   Monitoring is “systematic” if one or more of the following factors are present:

   - Occurring according to a system;
   - Pre-arranged, organised or methodical;
   - Taking place as part of a general plan for data collection;
   - Carried out as part of a strategy.

   “Large-scale processing” occurs if one or more of the following factors are present:

   - the number of data subjects concerned is large, either as a specific number or as a proportion of the relevant population;
   - the volume of data and/or the range of different data items being processed is large;
   - the duration, or permanence, of the data processing activity is large resp. long;
   - the geographical extent of the processing activity is large.

3. The core activities[4] of the processor consist of processing of special categories of data or personal data relating to criminal convictions and offences on a large scale.

   For the meaning of “large-scale processing”, please cf. the preceding enumeration point.

4. The processor is subject to the law of one or several Member States which requires it to designate a data protection officer (see in this respect the information at "relevant national law").

Details on the subject of the requirement:

1. The processor SHALL document the designation of the data protection officer.
2. The processor SHALL designate the data protection officer based on the following professional qualities:

   - Expertise in national and European data protection laws and practices including an in-depth understanding of the GDPR;
   - Understanding of the processing operations carried out;
   - Understanding of information technologies and data security;

[3] ‘Core activities’ can be considered as the key operations to achieve the processor’s objectives. These also include all activities where the processing of data forms as inextricable part of the processor’s activity.

[4] Cf. the previous footnote.

- Knowledge of the business sector and the organisation;
- Ability to promote a data protection culture within the organisation;
- Ability to fulfil DPO tasks.

3. The processor SHALL
   - publish the contact details of the data protection officer, thereby ensuring that data subjects can contact the DPO;
   - communicate the contact details of the DPO to the competent supervisory authority, thereby ensuring that supervisory authorities can contact the DPO.
4. The processor SHALL ensure that the data protection officer:
   - is involved, from an early stage, in all issues which relate to the protection of personal data, especially concerning the processing operations to be certified;
   - has time, financial resources, and access to tools/departments and documents to carry out their tasks and to maintain their expert knowledge;
   - can act in an independent manner, does not receive any instructions regarding the exercise of their legal tasks and is not dismissed or penalised for performing these tasks;
   - can report regularly and directly to the highest management level of the processor;
   - is not involved in any tasks and duties that leads them to determine the purpose and the means of the processing of personal data and would thus result in a conflict of interest;
   - cooperates with the competent supervisory authority and acts as a contact point to facilitate access by supervisory authorities to the documents, information as well as for exercise of their investigative, corrective and advisory powers (cf. also chapter 1.1.4 below).

Relevant national law (if applicable):

DE: Section 38 par. 1 of the Federal Data Protection Act (BDSG) stipulates an obligation to designate a DPO for non-public bodies if at least one of the following constellations exists: The processor

- constantly employs as a rule at least 20 persons dealing with the automated processing of personal data.
- undertakes processing subject to a data protection impact assessment, or
- commercially processes personal data for the purpose of transfer, of anonymized transfer or for purposes of market or opinion research.

1.1.3. Designation of a representative in the European Union

Requirement in a nutshell:

If the processor does not have an establishment in the European Union (EU) resp. the European Economic Area (EEA), it SHALL have designated in writing a representative in the EU if the processing operations to be certified are covered by the territorial scope of the GDPR pursuant to its Art. 3 par. 2 and neither of the two exceptional cases listed in Art. 27 par. 2 GDPR apply.

Requirement in detail:

Conditions for / exceptions to the applicability of the requirement:

If the processor is not established in the EU, it SHALL in principle appoint a representative in the EU if it processes personal data of data subjects who are in the Union and the processing is related to at least one of the following two constellations:

1. The processor offers goods or services to data subjects in the Union,
2. The processor monitors the behaviour of data subjects as far as their behaviour takes place within the Union.

However, the obligation to designate does not apply if at least one of the following two exceptions is relevant (cf. Art. 27 par. 2 GDPR):

1. The processing operations to be certified
    - are only occasionally[5],
    - do not include, on a large scale, processing of special categories of personal data or personal data relating to criminal convictions and offences; and
    - are unlikely to result in a risk to the rights and freedoms of natural persons, taking into account the nature, context, scope and purposes of the processing.
2. The processor is a public authority or body.

Details on the subject of the requirement:

The following individual requirements SHALL be met:

1. The processor SHALL designate the representative in the EU in writing.
2. The representative designated by the processor SHALL be established in one of the Member States where the data subjects, whose personal data are processed in relation to the offering of goods or services to them, or whose behaviour is monitored, are.
3. The processor SHALL have mandated the representative in the EU to be addressed in addition to or instead of the processor by, in particular, supervisory authorities and data subjects, on all issues related to the processing operations concerned, for the purposes of ensuring compliance with the GDPR. It must also have documented this accordingly.

In addition, it must be recalled that

- Whenever a transfer within the meaning of Art. 44 GDPR to a processor established outside the EU or the EEA takes place, the obligations stipulated in Chapter V of the GDPR must be fully respected;
- The present certification scheme is not a scheme pursuant to Article 46(2)(f) GDPR;

[5] Here, it is to be noted that it is very unlikely that a processor will have processing operations certified that are only occasionally.

- If certification is granted, the processor is not entitled to make use of the certification in a way that could give the impression that the certification itself is a transfer tool pursuant to Article 46(2)(f) GDPR.

Relevant national law (if applicable):

N/A

1.1.4. Cooperation with the supervisory authority

Requirement in a nutshell:

The processor SHALL comply with the obligation to cooperate with the competent supervisory authority as outlined below at “Requirement in detail”.

Requirement in detail:

Conditions for / exceptions to the applicability of the requirement:

This requirement is always applicable.

Details on the subject of the requirement:

1. The processor SHALL designate at least one person competent for cooperation with the competent supervisory authority. If the processor is obliged to designate a data protection officer (cf. already chapter 1.1.2 above), they SHALL comply with option 1 below. If the processor is not obliged to designate a DPO, they SHALL comply either with option 1 or with option 2 below.

   Option 1 (DPO):

   The processor SHALL

   a) designate a data protection officer who is the main contact point for cooperation with the competent supervisory authority;

   b) communicate the contact details of the DPO to the competent supervisory authority;

   c) communicate changes to the competent supervisory authority, if a new DPO were to be appointed.

   Option 2 (other point of contact than DPO):

   The processor SHALL

   a) designate an employee or a service provider to be the main contact point for cooperation with the competent supervisory authority and to be in charge of any tasks relating to cooperation with the supervisory authority;

   b) make clear, in the communications with supervisory authorities and public, that this person is not a data protection officer.

2. The processor SHALL publish the contact details of the main contact point for cooperation with the competent supervisory authority to ensure that supervisory authorities can reach them.

3. The processor SHALL ensure by means of an implemented process that the DPO / other main contact point cooperates with the competent supervisory authority and acts as a contact point on issues relating to processing of personal data, and to

facilitate access by the supervisory authority to the documents, information as well as for exercise of their investigative, corrective and advisory powers.

Relevant national law (if applicable):

N/A

1.2. Requirements with regard to Art. 28 GDPR (relationship processor - controller)

1.2.1. Existence of contractual clauses that meet all the requirements of Art. 28 GDPR

Requirement in a nutshell:

Scenario 1: Processor acts for a large number of controllers

The processor SHALL have a template for a data processing agreement (DPA) with its principals (controllers) that meets all requirements of Art. 28 GDPR. The processor SHALL submit the contract template to the certification body as proof of this. In this respect, individually created templates and standard contractual clauses[6] (cf. Art. 28 par. 6-8 GDPR) can be considered.

In addition, the processor SHALL submit actual contracts based on the template and signed by both parties to the certification body.

It is necessary to clarify that the template for a data processing agreement is without prejudice to the right of the controller to provide or negotiate the Art. 28 GDPR clauses with the processor, without consequences on the certification.

Scenario 2: Processor only acts for one / a few controller(s)

The processor SHALL have concluded a contract with each controller that meets the requirements of Art. 28 GDPR. The signed contract[7] must be submitted to the certification body as proof of this.

Requirement in detail:

Conditions for / exceptions to the applicability of the requirement:

This requirement is not applicable if the respective processing by a processor on behalf of the controller is not based on a contract but on another legal instrument under Union or Member State law.

Details on the subject of the requirement:

To scenario 1 (standard contractual clauses):

[6] In June 2021, the European Commission published standard contractual clauses pursuant to Art. 28 par. 7 GDPR that meet the requirements for contracts between controllers and processors pursuant to Art 28 par. 3 and 4 GDPR. These clauses can be found in the Annex to the corresponding Commission Implementing Decision (EU) 2021/915, which has been effective since 27.06.2021.

[7] Only the contract clauses relevant from a data protection perspective need to be submitted. If the respective contract contains other clauses that are not relevant from a data protection perspective, these do not have to be submitted resp. the corresponding passages can be blacked out.

The processor SHALL adopt the standard contractual clauses and ensure that no conflicting clauses are included. It SHALL fill in the annexes / free text fields of the standard contractual clauses that need to be completed.

The processor SHALL specify in a work instruction or similar how it ensures that the requirements of Art. 28 GDPR are complied with if the standard contractual clauses are not concluded in individual cases because the controller does not agree to their use.

To scenario 1 (contract template) and to scenario 2 (contracts with the controller(s)):

1. The contract resp. contract template SHALL be binding on the processor with regard to the controller and set out the:

   a) Subject-matter and duration of the processing

      The subject-matter of the processing SHALL be specified. In this respect, it may be referred to the relevant passages of a possible "main contract" (in the sense of a service level agreement - SLA). However, such a reference SHALL then be so specific that these passages can be found without further ado.

      The exact time period or the criteria according to which it is determined SHALL be specified. This is particularly ensured if either the planned start and end of the processing are indicated or it is specified that the contractual relationship is entered into for an indefinite period of time, whereby in the latter case information must then also be provided on the period of notice.

   b) Nature and purpose of the processing

      The description of the nature and purpose SHALL be made in relation to the specific processing operation.

   c) Type of personal data

      In this respect, it SHALL in particular also be indicated whether special categories of personal data (cf. Art. 9 GDPR) are processed and, if so, which special categories exactly are concerned (e.g. health data or genetic data). If personal data on criminal convictions and offences or traffic and/or location data as defined by the ePrivacy Directive are processed, this SHALL also be indicated.

   d) Categories of data subjects

      Blanket statements such as "contractual or business partners" are to be avoided. Instead, specific categories SHALL be designated[8], such as: customers, suppliers, prospects, users of a service, subscribers, visitors, passers-by, patients or employees. The higher the risk of the data processing in question, the more precise the categories SHALL be designated.

   e) Obligations and rights of the controller

      The obligations of the controller arise in particular from chapters III and IV of the GDPR. With regard to its rights, the rights of instruction and control are to be mentioned in particular.

[8] The only exception is when the categories of data subjects cannot be narrowed down due to the nature of the processing operations concerned.

2. The contract or contract template SHALL also stipulate that:

   a) The processor processes the personal data only on documented instructions[9] from the controller (including with regard to transfers of personal data to a third country or an international organisation), unless required to do so by Union or Member State law[10] to which it is subject and that, if it is subject to such an obligation, it SHALL inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest.

   b) The processor ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under a statutory obligation of confidentiality.

      If statutory confidentiality obligations or professional secrets and special official secrets which are not based on statutory provisions are relevant, chapter 1.4.1 of these criteria is also to be observed, according to which the contract / contract template SHALL address the corresponding confidentiality obligation. Insofar as the applicable Union or Member State law provides that the processor is to be obliged by the controller to maintain confidentiality with regard to the relevant confidentiality obligation and to be made aware of the consequences of a possible breach of this obligation, this SHALL also be addressed in the contract / the contract template.

   c) The processor takes all measures required pursuant to Art. 32 GDPR. Specifically, this means the following:

      The contract / contract template SHALL contain information on the measures to be taken or already implemented or refer to a separate document listing the TOM.[11] The contractual clauses SHALL provide for an obligation for the processor to obtain the consent of the controller before making any substantial changes to the measures, as well as for a regular review of the TOM to ensure their appropriateness in view of the risks that may develop over time.

   d) The processor respects the conditions referred to in Art. 28 par. 2 and par. 4 sentence 1 GDPR for engaging another processor.

      In this respect, different variants come into consideration. The processor SHALL make specifications in the contract / contract template regarding the relevant variant in the individual case:

      Variant 1: The use of other processors is generally excluded.

      Variant 2: The processor shall not engage other processors without prior specific written authorisation (electronic format is sufficient) of the controller.

      Variant 3: The controller issues a general written (electronic format is sufficient)

[9] Instructions are documented if their content is recorded in electronic or written form. This means that verbal instructions are also permissible, provided they are documented subsequently.

[10] In this respect, provisions of the respective national law on internal security come into consideration in particular: Example with regard to DE: § 22 a par. 5 BPolG.

[11] Irrespective of this, successful certification is only ever possible if the relevant measures have been implemented (cf. chapter 2 below).

authorisation for the use of other processors. In this case, the processor shall inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes.

If the contract / contract template is designed to authorise certain other processors at the time of signing the agreement, a list of the authorised other processors SHALL be included in the contract or an annex thereto.

e) The processor, taking into account the nature of the processing, assists the controller by technical and organisational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in chapter III of the GDPR.[12]

While in some constellations the assistance may simply consist in forwarding any request received without delay and/or enabling the controller to directly extract and manage the relevant personal data, in certain circumstances more specific, technical tasks may be assigned to the processor. This is particularly the case if the processor is able to extract and manage the personal data.

In this respect, it must be taken into account to what extent the controller is actually dependent on the processor for the assistance of the processor regarding data subject rights.

Such clauses should be in line with the GDPR responsibility of the controller regarding data subject rights and not unduly transfer this responsibility to the processor.

f) The processor assists the controller in ensuring compliance with the obligations pursuant to Art. 32 to 36 GDPR, taking into account the nature of processing and the information available to the processor.

Specifically, this involves assisting the controller with regard to the following obligations:

- Obligation to implement technical and organisational measures;
- Obligation to notify personal data breaches to the supervisory authority and to the data subjects;
- Obligation to carry out a data protection impact assessment if required and to consult the supervisory authority where the DPIA indicates that there is a high risk that cannot be mitigated.

g) The processor, at the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies unless Union or Member State law requires storage of the personal data.

As a result, the processor SHALL ensure in this respect that after the end of the provision of services relating to processing, no personal data remain with the

[12] The support services available to the processor depend on the type of processing. In this respect, see also chapter 3 of these criteria.

processor which have been provided to it for the purpose of order fulfilment and for which there are no legal storage obligations (any more). This also includes the deletion / return of any copies made.

h) The processor makes available to the controller all information necessary to demonstrate compliance with the obligations laid down in Art. 28 GDPR[13] and allows for and contributes to audits[14], including inspections, conducted by the controller or another auditor mandated by the controller.

i) The processor shall immediately inform the controller if, in its opinion, an instruction infringes the GDPR or other Union or Member State data protection provisions.

3. The following further requirement only concerns scenario 1 (contract template): The processor SHALL specify in a work instruction or similar how it is ensured that the requirements of Art. 28 GDPR are complied with if the contract template is not used in an individual case because the controller does not agree to this.

Relevant national law (if applicable):

1. If applicable: §§ regarding other legal instruments (→ Art. 28 par. 3 sentence 1 GDPR)
2. If applicable: §§ of internal security law etc. (→ Art. 28 par. 3 sentence 2 lit. a) GDPR)
3. If applicable: Legal storage obligations (→ Art. 28 par. 3 sentence 2 lit. g) GDPR)
4. If applicable: National law relevant with regard to the lawfulness of an instruction (→ Art. 28 par. 3 sentence 3 GDPR)

1.2.2. Implementation of the contractually agreed duties: Responsibilities, processes, work instructions

Requirement in a nutshell:

The processor SHALL have implemented measures to comply with the obligations agreed in the contract resp. provided for in the contract template (cf. below at “Requirement in detail”).

Requirement in detail:

Conditions for / exceptions to the applicability of the requirement:

This requirement is always applicable when certifying processing operations by processors.

Details on the subject of the requirement:

The processor SHALL have implemented measures to comply with resp. implement the contractually agreed obligations. In particular, when reviewing compliance with the individual requirements listed below, documents that define responsibilities and processes resp. that

[13] See also chapter 1.2.2 of these criteria (under details on the subject of the requirement, no. 8).

[14] Here, it must be specified how the processor enables audits by the controller or third parties commissioned by the controller and how it (actively) contributes to them. This includes on-site audits and / or inspections of IT systems and procedures.

deal with work instructions or confidentiality obligations of the processor's employees are to be considered.

Specifically, the processor SHALL demonstrate that it has implemented measures to comply with the contractual agreements on the following topics:

1. Process personal data only on documented instructions from the controller, unless required to do so by Union or Member State law.

   In this respect, the processor SHALL especially specify which persons / departments are authorised to receive instructions from the controller.

2. Confidentiality commitments of the persons authorised to process the personal data resp. the existence of a statutory obligation of confidentiality of these persons.

   In this respect, the processor SHALL submit to the certification body templates currently in use for confidentiality resp. secrecy obligations of the relevant personnel.

3. Implement all measures required pursuant to Art. 32 GDPR (→ this is addressed by the requirements of chapter 2 of these criteria).

4. Compliance with the conditions for engaging another processor.[15]

   The processor SHALL specify responsibilities and processes in work instructions and/or other documents. These SHALL comply with the respective contractual agreements with the controller(s) – cf. chapter 1.2.1.2.d) above.

5. Assist the controller in responding to requests to exercise data subjects' rights.[16]

   The activities required in this respect result from the relevant contractual clauses with the controller(s) - cf. chapter 1.2.1.2.e) above.[17]

6. Assist the controller in ensuring compliance with the obligations pursuant to Art. 32-36 GDPR.

   The activities required in this respect result from the relevant contractual clauses with the controller(s) – cf. chapter 1.2.1.2.f) above. In this respect, a differentiation is to be made as follows:

- Art. 32 GDPR: This is addressed by chapter 2 of these criteria.
- Art. 33 f. GDPR: The processor SHALL have implemented measures to ensure that it notifies the controller without undue delay after becoming aware of a personal data breach (cf. Art. 33 par. 2 GDPR). The measures implemented by the processor to comply with the contractually agreed obligations to support the controller in notifying

[15] With regard to other processors actually used, it must also be examined whether further requirements are met in the specific case. For example, it must be checked whether the contractual obligations in the relationship between the controller and the processor are "passed on" to the other processor (cf. Art. 28 par. 4 sentence 1 GDPR) and whether the latter has implemented technical and organisational measures within the meaning of Art. 32 GDPR. This is addressed in the next chapter and in chapter 2 of these criteria.

[16] This is the addressed by chapter 3 of these criteria.

[17] While the assistance may simply consist in promptly forwarding any request received and/or enabling the controller to directly extract and manage the relevant personal data, in some circumstances the processor will be given more specific, technical duties, especially when it is in the position of extracting and managing the personal data (EDPB, Guidelines 07/2020).

data subjects in accordance with Art. 34 GDPR and, if applicable, other relevant support obligations are also covered by this requirement.

- Art. 35 f. GDPR: The processor SHALL also in this respect have implemented all measures necessary to comply with the contractually agreed obligations. If controllers are obliged to carry out a data protection impact assessment when using the processing operations to be certified as intended, the processor SHALL also carry out an exemplary DPIA[18] in the sense of a broad interpretation of the principles of data protection by design and by default, document its results and make them available to the controllers (in this way, the processor provides preparatory work that supports the controllers in complying with their obligations pursuant to Art. 35 GDPR, whereby the processor in turn provides assistance in compliance with Art. 28 par. 3 sentence 2 lit. f) GDPR).

7. Delete or return all personal data after the end of the provision of processing services, unless Union or Member State law requires storage of the personal data.[19]
8. To provide all necessary information to demonstrate compliance with Art. 28 GDPR as well as allowing for and contributing to audits, including inspections, conducted by the controller or another auditor mandated by the controller.

   In respect of the provision of all necessary information to demonstrate compliance with Art. 28 GDPR, the processor SHALL submit the following documentation to the certification body:

   a) "TOM document" - description of the implemented technical and organisational measures,
   b) Work instructions / process descriptions to ensure compliance with DPA clauses:
      a. Document re how to handle instructions by the controller
      b. Proof re commitments to confidentiality
      c. Work instruction/s re the engagement of other processors
      d. Work instruction/s re data subject requests
      e. Work instruction re personal data breaches
   c) Relevant documents resp. information on the topic of other processors (if relevant – cf. also chapter 1.3):
      a. List of other processors with ToE relevance and their location
      b. Document re the selection of other processors in general
      c. Document/s demonstrating careful selection of each other processor
      d. Signed data protection agreement/s with other processors (DPA)

[18] Even though an exemplary DPIA is mentioned here, this does not mean that the processor itself must carry out a DPIA in accordance with Article 35 GDPR. Rather, what is meant is that the processor prepares a document on the risks of the processing operations to be certified before being commissioned by a specific controller, which it then makes available to the controller after having been commissioned. The controller is thus supported by the preparatory work of the processor in carrying out a DPIA.

[19] The technical requirements that have to be met with regard to deletion are addressed in chapter 2.1.6 of these criteria.

c) Relevant documents resp. information on the topic of "transfer of personal data to a third country" (if relevant – cf. also chapter 1.4.2)

a. Results of transfer impact assessment/s (TIA)
b. Other documents related to a transfer to a third country
    i. Binding corporate rules and proof of their approval
    ii. Standard data protection clauses used
    iii. Codes of conduct and proof of their approval
    iv. Documents relating to certification in accordance with Art. 42 GDPR
    v. Documents relating to one of the derogations listed in Art. 49 GDPR
    vi. Evidence with regard to implemented supplementary measures

d) If applicable, relevant log data documenting compliance with the requirements of the GDPR,

e) If applicable, information on adherence to approved codes of conduct resp. approved certification mechanisms,

f) If applicable, information on other relevant certifications / audits or inspections.

9. Inform the controller if, in the processor's opinion, an instruction infringes the GDPR or other Union or Member State data protection provisions.

   The process defined by the processor in this respect must also specify how instructions are specifically dealt with, the implementation of which leads to flagrant violations of the law and/or serious violations of the personal rights of the data subjects.

Relevant national law (if applicable):

1. If applicable: §§ regarding other legal instruments (→ Art. 28 par. 3 sentence 1 GDPR)
2. If applicable: §§ of internal security law etc. (→ Art. 28 par. 3 sentence 2 lit. a) GDPR)
3. If applicable: Legal storage obligations (→ Art. 28 par. 3 sentence 2 lit. g) GDPR)
4. If applicable: National law relevant with regard to the lawfulness of an instruction (→ Art. 28 par. 3 sentence 3 GDPR)

1.3. Requirements with regard to Art. 28 GDPR (relationship processor - other processor)

This subchapter is applicable whenever the certification customer (processor) makes use of other processors. The notion "other processor" refers to cases where the certification customer engages another processor.

Since a reliable statement as to whether EU data protection law is complied with in respect of the processing operations to be certified can only be made if the other processors are also considered, the following requirements are always applicable in such cases.[20]

1.3.1. Selection of other processors with regard to data protection guarantees

Requirement in a nutshell:

The processor SHALL have established and documented a process (e.g. in a work instruction / process description) on how to proceed when selecting other processors.

For each other processor involved in the provision of the processing operations to be certified, the processor SHALL demonstrate that it has selected the other processor with regard to data protection guarantees as further specified below at “Requirement in detail”.

Requirement in detail:

Conditions for / exceptions to the applicability of the requirement:

This requirement shall apply in the case of a certification of processing operations by processors where the processor relies on other processors involved in the provision of the processing operations to be certified.

Details on the subject of the requirement:

If the processor wishes to use the services of other processors, it SHALL satisfy itself when selecting them that they provide guarantees that technical and organisational measures will be implemented in such a way that the processing will be carried out in compliance with the requirements of the GDPR and will ensure the protection of the rights of the data subjects. The criteria to be taken into account when selecting a potential other processor are, in particular, its expert knowledge, reliability and resources (cf. recital 81 sentence 1 of the GDPR); in addition, its financial stability and reputation may also be taken into account.

Adherence to an approved code of conduct or an approved certification mechanism by another processor may be used as an element to demonstrate its careful selection by the processor (cf. recital 81 sentence 2 of the GDPR).[21] However, recognised international certifications such as the ISO/IEC 27000 series, results of external or internal audits, control options resp. audit rights of the processor, contractual assurances, individual security concepts, TOM documents or other documents that may be relevant with regard to the existence of guarantees (e.g. an information security policy or a record of processing activities) may also be relevant as evidence.

The processor SHALL select from the means of proof listed above those which are appropriate to the risks associated with the processing activities of the other processor.

Note: Sub-processors must always be selected based on several of the elements listed above. By contrast, it is not sufficient to only rely on one of these elements.

[20] In principle, all other processors involved are to be considered. If the processor uses the services of several other processors who perform similar activities (e.g. translation agencies), an exemplary check (closer examination of only one resp. a few of these other processors as part of the evaluation) may be sufficient in the context of a certification procedure. However, this is only the case if this has been made clear in the evaluation concept.

[21] This, of course, is always subject to the condition that the services provided by the other processor to the processor are covered by the scope of the certification resp. code of conduct.

Important:

Chapter 2 then examines the technical and organisational measures implemented at other processors with regard to the specific requirements listed there (insofar as these are relevant with regard to the services provided by the respective other processor).

Relevant national law (if applicable):

N/A

1.3.2. Existence of signed data processing agreements with all other processors

Requirement in a nutshell:

The processor SHALL have concluded contracts with all other processors that impose the same data protection obligations as set out in the contract(s) between the controller(s) and the processor on that sub-processor. The signed contract SHALL be[22] submitted to the certification body as proof of this in each case.

Requirement in detail:

Conditions for / exceptions to the applicability of the requirement:

This requirement shall be applicable in the case of certification of processing operations by processors where the processor engages other processors.

Details on the subject of the requirement:

1. The processor SHALL have concluded a data processing agreement with each other processor containing binding provisions on the following aspects:

a) Subject matter and duration of processing

   The subject matter of the contract SHALL be specified. In this respect, it may be sufficient to refer to the relevant passages of a possible "main contract" (in the sense of a service level agreement - SLA). However, such a reference SHALL then be so specific that these passages can be found without further ado.

   The exact time period or the criteria according to which it is determined SHALL be specified. This is particularly ensured if either the planned start and end of the processing are indicated or it is specified that the contractual relationship is entered into for an indefinite period of time, whereby in the latter case information must then also be provided on the period of notice. These specifications on the duration of the processing shall be in accordance with the relevant provisions of the data processing agreement between the controller and the processor / the respective contract template.

b) Nature and purpose of the processing

   The description of the nature and purpose SHALL be made in relation to the specific processing operation.

[22] Only the contract clauses relevant from a data protection perspective need to be submitted. If the respective contract contains other clauses that are not relevant from a data protection perspective, these do not have to be submitted resp. the corresponding passages can be blacked out.

c) Type of personal data

In this respect, it SHALL in particular also be indicated whether special categories of personal data (cf. Art. 9 GDPR) are processed and, if so, which special categories exactly are concerned (e.g. health data or genetic data). If personal data on criminal convictions and offences or traffic and/or location data as defined by the ePrivacy Directive are processed, this SHALL also be indicated.

d) Categories of data subjects

Blanket statements such as "contractual or business partners" are to be avoided. Instead, specific categories SHALL be designated[23], such as: customers, suppliers, prospects, users of a service, subscribers, visitors, passers-by, patients or employees. The higher the risk of the data processing in question, the more precise the categories SHALL be designated.

e) Obligations and rights of the processor in relation to the other processor

With regard to the rights of the processor in relation to the other processor, the rights of instruction and control are to be mentioned in particular.

2. The contract SHALL also stipulate that:

a) The other processor processes the personal data only on documented instructions[24] from the processor (including with regard to transfers of personal data to a third country or an international organisation), unless required to do so by Union or Member State law[25] to which it is subject and that, if it is subject to such an obligation, it SHALL inform the processor of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest.

b) The other processor ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under a statutory obligation of confidentiality.

If statutory confidentiality obligations or professional secrets and special official secrets which are not based on statutory provisions are relevant, chapter 1.4.1 of these criteria must also be observed, according to which the contract SHALL address the corresponding confidentiality obligation. Insofar as the applicable Union resp. Member State law provides that the other processor is to be obliged to maintain confidentiality with regard to the relevant confidentiality obligation and to be made aware of the consequences of a possible breach of this obligation, this SHALL also be addressed in the contract.

c) The other processor takes all measures required pursuant to Art. 32 GDPR. Specifically, this means the following:

The contract SHALL contain information on the measures to be taken resp. already

[23] The only exception is when the categories of data subjects cannot be narrowed down due to the nature of the processing operations concerned.

[24] Instructions are documented if their content is recorded in electronic or written form. This means that verbal instructions are also permissible, provided they are documented subsequently.

[25] In this respect, provisions of the respective national law on internal security come into consideration in particular: Example with regard to DE: § 22 a par. 5 BPolG.

implemented or refer to a separate document listing the TOM.[26] It SHALL provide for an obligation for the other processor to obtain the consent of the processor before making any substantial changes to the measures, as well as for a regular review of the TOM to ensure their adequacy in view of risks that may develop over time.

d) The other processor respects the conditions referred to in Art. 28 par. 2 and par. 4 sentence 1 GDPR for engaging additional other processors.

   In this respect, different variants come into consideration. The contract SHALL specify which variant is relevant in the individual case:

   Variant 1: The use of additional other processors is generally excluded.

   Variant 2: The other processor shall not engage additional other processors without prior specific written authorisation (electronic format is sufficient) of the processor.

   Variant 3: The processor issues a general written (electronic format is sufficient) authorisation for the use of additional other processors. In this case, the other processor shall inform the processor of any intended changes concerning the addition or replacement of additional other processors, thereby giving the processor the opportunity to object to such changes.

   If the contract is designed to authorise certain additional other processors at the time of signing the agreement, a list of the authorised additional other processors SHALL be included in the contract or an annex thereto.

e) The other processor, taking into account the nature of the processing, assists the processor by technical and organisational measures in fulfilling its duty to assist the controller in complying with its obligation to respond to requests for exercising the data subject's rights laid down in chapter III of the GDPR.[27]

f) The other processor assists the processor in fulfilling its duty to assist the controller in complying with the obligations referred to in Articles 32 to 36 GDPR, taking into account the nature of processing and the information available to the other processor.

   Specifically, this involves assisting the processor in assisting the controller with regard to the following obligations:

- Obligation to implement technical and organisational measures.
- Obligation to notify personal data breaches to the supervisory authority and to the data subjects.
- Obligation to carry out a data protection impact assessment if required and to consult the supervisory authority where the DPIA indicates that there is a high risk that cannot be mitigated.

g) The contract SHALL provide that the other processor, at the choice of the processor, deletes or returns all the personal data to the processor after the end of the provision of services relating to processing, and deletes existing copies unless Union or Member State law requires storage of the personal data.

[26] Irrespective of this, successful certification is only ever possible if the relevant measures have been implemented (cf. chapter 2 below).

[27] The support services that may be provided by the other processor depend on the type of processing.

Note: The choice of the processor SHALL be made in accordance with the choice made by the controller vis-à-vis the processor.[28]

As a result, it SHALL be ensured that after the end of the provision of services relating to processing, no personal data remain with the other processor which have been provided to it for the purpose of order fulfilment and for which there are no legal storage obligations (any more). This also includes the deletion / return of any copies made.

h) The other processor makes available to the processor all information necessary to demonstrate compliance with the obligations laid down in Art. 28 GDPR[29] and allows for and contributes to audits[30], including inspections, conducted by the processor or another auditor appointed by the processor resp. directly by the controller.

i) The other processor shall immediately inform the processor if, in its opinion, an instruction infringes the GDPR or other Union or Member State data protection provisions.

Relevant national law (if applicable):

1. If applicable: §§ regarding other legal instruments (→ Art. 28 par. 3 sentence 1 GDPR)
2. If applicable: §§ of internal security law etc. (→ Art. 28 par. 3 sentence 2 lit. a) GDPR)
3. If applicable: Legal storage obligations (→ Art. 28 par. 3 sentence 2 lit. g) GDPR)
4. If applicable: National law relevant with regard to the lawfulness of an instruction (→ Art. 28 par. 3 sentence 3 GDPR)

1.3.3. Implementation of the contractually agreed duties: Responsibilities, processes, work instructions

Requirement in a nutshell:

The processor SHALL have implemented measures to comply with the obligations agreed in the contract.

Requirement in detail:

Conditions for / exceptions to the applicability of the requirement:

This requirement shall be applicable in the case of certification of processing operations by processors where the processor engages other processors.

Details on the subject of the requirement:

[28] In this respect, cf. chapter 1.2.1.

[29] Information in this sense includes all documents/data that enable the processor to verify compliance with the GDPR by the other processor. This includes, for example, a data protection concept (if available), a document describing the technical and organisational measures implemented, information on any additional other processors and any transfers to third countries, as well as log data that provide information on compliance with certain provisions of the GDPR.

[30] In this respect, it must be specified how the other processor enables audits by the processor or third parties commissioned by the processor resp., if applicable, also directly by the controller and how it (actively) contributes to them. This includes on-site audits and / or inspections of IT systems and procedures.

The processor SHALL demonstrate that it has implemented measures to comply with the contractual agreements with the other processors on the following topics:

1. Process personal data only on documented instructions from the processor, unless the other processor is required to do so by Union or Member State law.

   The processor SHALL specify which persons resp. departments are authorised to give instructions in relation to the other processor. In addition, the extent to which an authorisation to issue individual instructions exists and how (i.e. in what form) these are to be issued and documented SHALL be specified in a work instruction or similar in accordance with the contractual provisions.

2. Compliance with the conditions for engaging additional other processors as contractually agreed between the processor and the other processor – cf. chapter 1.3.2.2.d) above.

   The processor SHALL specify which persons or departments are authorised to separately approve resp. object to the use of additional other processors by the other processor, unless the engagement of other processors has been contractually excluded.

3. Assist the processor in assisting the controller in responding to requests for the exercise of data subject rights as contractually agreed between the processor and the other processor – cf. chapter 1.3.2.2.e) above.

   The processor SHALL specify which persons resp. departments are the contact persons of the other processor in this respect and may request the corresponding support services from the other processor.

4. Assist the processor in assisting the controller in ensuring compliance with the obligations pursuant to Art. 32-36 GDPR as contractually agreed between the processor and the other processor – cf. chapter 1.3.2.2.f) above.

   The processor SHALL specify to which persons resp. departments the other processor has to notify a personal data breach and how to deal with such notifications (→ informing the controller(s), etc.). If the topic of data protection impact assessment is relevant, responsibilities and processes must also be specified with regard to requesting, receiving and taking into account related support services from the other processor.

5. Delete or return all personal data after the end of the provision of processing services, unless Union or Member State law requires storage of the personal data.

   The processor SHALL also implement measures to implement the contractual provisions in this respect.[31]

6. Inform the processor if, in the opinion of the other processor, an instruction infringes the GDPR or other Union or Member State data protection provisions.

   The processor SHALL specify which persons resp. departments the other processor

[31] e.g., specify which persons resp. departments are authorised to require the other processor to delete or return personal data and/or to require the production of records of the deletion/destruction of personal data, in accordance with the choice made by the controller in this regard.

shall inform if it considers an instruction from the processor to infringe data protection provisions and how these persons or departments have to deal with this.

Relevant national law (if applicable):

1. If applicable: §§ regarding other legal instruments (→ Art. 28 par. 3 sentence 1 GDPR)
2. If applicable: §§ of internal security law etc. (→ Art. 28 par. 3 sentence 2 lit. a) GDPR)
3. If applicable: Legal storage obligations (→ Art. 28 par. 3 sentence 2 lit. g) GDPR)
4. If applicable: National law relevant with regard to the lawfulness of an instruction (→ Art. 28 par. 3 sentence 3 GDPR)

1.4. Requirements for specific types of processing operations

The subsequent requirements relate to the following topics:

- Statutory confidentiality obligations / professional and special official secrets and
- Transfer of personal data to third countries.

1.4.1. Statutory confidentiality obligations as well as professional secrets and special official secrets not based on statutory provisions

Requirement in a nutshell:

If the processing operations to be certified are exclusively resp. predominantly (> 50%) used by controllers who are subject to specific confidentiality obligations under EU or relevant Member State law, the processor SHALL take this into account in the relationship with the controllers and with any other processors.[32]

Requirement in detail:

Conditions for / exceptions to the applicability of the requirement:

This requirement is only applicable if the processing operations to be certified are exclusively resp. predominantly (> 50%) used by controllers who are subject to special confidentiality / secrecy obligations.

Details on the subject of the requirement:

In this respect, a distinction must be made between the constellations described below:

1. The following shall apply in relation to controllers, who are subject to a special confidentiality obligation:

[32] Even if certification on the basis of these criteria (only) serves the purpose to demonstrate that processing operations by processors comply with EU data protection law, it would be unacceptable if any relevant confidentiality obligations (e.g. in the case of processing operations in the health sector) were not taken into account in the context of certification because of the close connection between EU data protection law and the specific confidentiality obligations.

- The contract template for a data processing agreement to be provided by the processor resp. the contracts concluded with individual controllers[33] SHALL address the specific confidentiality obligation.[34]
- To the extent that the applicable Union resp. Member State law provides that the processor must be bound by the controller to maintain confidentiality with regard to the relevant confidentiality obligation and be made aware of the consequences of any breach of this obligation, this SHALL also be the subject of the contract template for a data processing agreement to be provided by the processor resp. of the contracts concluded with individual controllers.

2. In relation to other processors (in particular sub-processors) to whom personal data subject to a special confidentiality obligation are disclosed, the following shall apply:

- The relevant specific confidentiality obligation SHALL be addressed in the respective data processing agreement.[35]
- To the extent required by Union resp. Member State law, the processor SHALL impose confidentiality obligations on other processors involved in the processing operations to be certified with regard to the relevant confidentiality obligation and inform them of the consequences of any breach of this obligation.
- Where applicable, other requirements of EU resp. Member State law SHALL be observed.

Relevant national law:

DE: Section 203 StGB, Sections 1 par. 2 sentence 3 as well as 22 and 29 of the Federal Data Protection Act (BDSG)[36]

1.4.2. Transfer of personal data to third countries

First of all, it must be noted that the EuroPriSe certification scheme for processors itself is not a certification according to Article 46(2)(f) of the GDPR meant for international transfers of personal data and therefore does not provide appropriate safeguards within the framework of transfers of personal data to third countries or international organisations under the terms referred to in letter (f) of Article 46(2). Consequently, the processor (certification applicant) must inform the controller(s) about the fact that the EuroPriSe certification scheme for processors itself is not a transfer instrument according to Article

[33] Cf. chapter 1.2.1 of these criteria.

[34] Since this matter is largely regulated at national level, this requirement is formulated relatively vaguely. Its concrete implementation in practice then depends on the requirements that national law provides in this area. This is the case as long as there are no indications that data protection provisions are being restricted in an inadmissible way.

[35] Cf. the previous footnote and chapter 1.3.2 of these criteria.

[36] - Examples of statutory confidentiality obligations are Section 43a par. 2 BRAO and Section 62 StBerG.
- Examples of professional secrets that are not based on statutory confidentiality obligations are the medical secrecy obligation (cf. § 9 MBO-Ä) or the secrecy obligation for psychotherapists standardised in the corresponding professional regulations under state law.
- Examples of (legally regulated) special official secrets are tax secrecy (§ 30 AO) and social secrecy (§ 35 SGB V).

46(2)(f) of the GDPR. The specific requirements listed below are only applicable when the processor is transferring personal data to a data importer in a third country.

1.4.2.1. Existence of an adequacy decision / appropriate safeguards

Requirement in a nutshell:

If the processing operations to be certified involve a transfer of personal data to third countries resp. international organisations, the processor SHALL comply with the conditions laid down in chapter V of the GDPR.

Requirement in detail:

Conditions for / exceptions to the applicability of the requirement:

This requirement is only applicable if the controller's use of the processing operations to be certified results in a transfer of personal data to third countries or international organisations.

Details on the subject of the requirement:

The processor SHALL have performed a Transfer Impact Assessment (TIA) and provide the certification body with the results. When performing the Transfer Impact Assessment, the EDPB's Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data must be observed.

The processor SHALL ensure that, with regard to any transfer of personal data to third countries resp. international organisations, the conditions of chapter V of the GDPR are complied with in order not to undermine the level of protection of individuals provided by the GDPR.

According to chapter V of the GDPR, the following options in particular can be considered as legitimisation for a transfer of personal data to third countries:

1. Adequacy Decisions of the EU Commission pursuant to Art. 45 GDPR[37],
2. Binding corporate rules pursuant to Art. 46 par. 2 lit. b) read in conjunction with Art. 47 GDPR[38],

[37] Cf. https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en. So far, adequacy decisions on Japan and the United Kingdom have been issued on the basis of Art. 45 GDPR. However, the adequacy decisions adopted on the basis of Art. 25 par. 6 of Directive 95/46/EC, which remain in force until further notice pursuant to Art. 45 par. 9 GDPR, are also relevant. These are adequacy decisions regarding Andorra, Argentina, Guernsey, Faroe Islands, Isle of Man, Israel, Jersey, Canada (limited scope: commercial organisations), New Zealand, Republic of Korea, Switzerland and Uruguay. Status: 10/2022

[38] This instrument can be considered in particular in the relationship between a processor and another processor. However, this is only the case if both belong to the same group of undertakings or the same group of enterprises engaged in a joint economic activity and if binding corporate rules have been approved in relation to this group of undertakings or enterprises. Furthermore, it must always be ensured that the processing operations to be certified, which the customer provides as a processor, are covered by the scope of the binding corporate rules (BCR). The basic prerequisite for this is first of all that the binding corporate rules are so-called "BCR for processors" (cf. in this respect also Art. 4 par. 20 GDPR). Binding corporate rules approved according to Art. 26 par. 2 of Directive 95/46/EC remain valid until further notice pursuant to Art. 46 par. 5 sentence 1 GDPR. The EU Commission provides a list of all companies whose BCR were approved prior to 25 May 2018 on the internet. A list of all companies whose BCR have been approved since then can be found on the EDPB's website: https://edpb.europa.eu/our-work-tools/accountability-tools/bcr_en.

3. Standard data protection clauses pursuant to Art. 46 par. 2 lit c) and d) GDPR[39],
4. Approved codes of conduct pursuant to Art. 40 GDPR[40],
5. An approved certification mechanism pursuant to Art. 42 GDPR[41],
6. One of the exceptions under Art. 49 GDPR is relevant.

   If one of the exceptions under Art. 49 is relevant, the processor SHALL provide specific information to the certification body as to which situations and under which conditions they would rely on the specific exemption.

The processor SHALL substantiate and document their choice of a particular transfer tool pursuant to Chapter V of the GDPR.

With regard to the transfer tools provided for in Art. 46 GDPR and in particular with regard to standard data protection clauses, the following is to be noted:

Here, it SHALL be assessed (and documented) on a case-by-case basis and, as the case may be, in collaboration with the importer (recipient of the personal data in the third country), if there is anything in the law or practice of the third country that may impinge on the effectiveness of the appropriate safeguards contained in the transfer tools under Art. 46 GDPR. If this is the case, the processor SHALL implement (and document) supplementary measures that fill these gaps in the protection and bring it up to the level required by EU law. In this respect, technical measures, organisational measures and additional contractual measures can be considered, whereby it may be necessary to combine several of these measures in individual cases.

When implementing supplementary measures, the EDPB's Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data must be observed.

Important: Contractual and organisational measures alone will generally not overcome access to personal data by public authorities, as there will be situations where only technical measures might impede or render ineffective such access.

Relevant national law:

National law on the basis of Art. 49 par. 1 lit. d) + g) and par. 5, 85 par. 2 GDPR, if applicable.

---

[39] In June 2021, the European Commission published standard data protection clauses pursuant to Article 46 par. 2 lit. c) GDPR for transfers of personal data from controllers or processors located in the EU/EEA (or otherwise subject to the GDPR) to controllers or processors located outside the EU/EEA (and not subject to the GDPR). These clauses can be found in the Annex of the corresponding Commission Implementing Decision (EU) 2021/914, effective since 27.06.2021. They will replace the standard contractual clauses adopted under the previous Data Protection Directive 95/46/EC. Cf. in this respect also Art. 46 par. 5 GDPR as well as Art. 4 par. 4 of the Implementing Decision, according to which the existing standard contractual clauses will continue to provide appropriate safeguards within the meaning of Art. 46 par. 1 GDPR until 27 December 2022, provided the processing operations that are the subject matter of the contract remain unchanged and the reliance on those clauses ensures that the transfer of personal data is subject to appropriate safeguards (in this respect, in view of the Schrems II ruling of the ECJ (C-311/18), supplementary measures may also have to be implemented - the mere agreement of the clauses alone is not sufficient in such a case). This transitional provision covers all contracts concluded before 27 September 2021 on the basis of Decision 2001/497/EC or Decision 2010/87/EU.

[40] together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards

[41] cf. the previous footnote

1.4.2.2. Bound by instructions with regard to the transfer of personal data to third countries

Requirement in a nutshell:

The processor may only transfer personal data to third countries if this is done in accordance with the instructions of the controller. The relevant data processing agreement resp. the contract template used by the processor SHALL provide for this.

Requirement in detail:

Conditions for / exceptions to the applicability of the requirement:

This requirement is only applicable if the controller's use of the processing operations to be certified results in a transfer of personal data to third countries or international organisations.

Details on the subject of the requirement:

If the processor transfers personal data to third countries as part of the processing operations to be certified, the contract template for a contract pursuant to Art. 28 par. 3 GDPR used by the processor resp. the contracts concluded with individual controllers SHALL contain a passage stipulating that and to what extent resp. under what conditions the processor is permitted to do so. The same applies to contracts between the processor and other processors, if applicable.

Relevant national law:

N/A

1.5. Data protection by design and by default

This chapter concerns requirements stemming from the principles of data protection by design and by default. The GDPR only directly obliges the controller to comply with these principles. However, since the controller must not only take the principles into account when selecting (IT) products, but also when selecting suitable processors, processors are also indirectly addressed by the relevant Art. 25 GDPR.[42] Therefore, in the context of a certification of processing operations by processors, it must be examined whether the processing operations to be certified comply with the principles of data protection by design and by default.

1.5.1. Data protection by design

Requirement in a nutshell:

The processor SHALL take into account the principle of data protection by design. It can do this either by taking technical and organisational measures itself that are designed to implement the data protection principles of Art. 5 GDPR or by facilitating the controller to implement such measures by designing the processing operations to be certified accordingly. It SHALL, in the sense of continuous improvement in a management system, implement processes that ensure the consideration of the principle of data protection by design both at the time of the selection resp. determination of the means (planning phase)

[42] See also recital 78 of the GDPR.

and at the time of the actual processing. The respective processes and results shall be documented.

Concrete measures required in this respect are listed in chapter 2 of these criteria (technical and organisational measures).

Requirement in detail:

Conditions for / exceptions to the applicability of the requirement:

This requirement is always applicable. Depending on the nature of the processing operations to be certified, different measures can be considered in this respect. Therefore, the measures to be implemented must always be determined with regard to the specific target of evaluation.

Details on the subject of the requirement:

The processor SHALL design the processing operations to be certified in such a way that they make it easy for the controllers to implement the data protection principles of Art. 5 GDPR listed below:

- Lawfulness;
- Fairness;
- Transparency;
- Purpose limitation;
- Data minimisation;
- Accuracy;
- Storage limitation;
- Integrity and confidentiality;
- Accountability.

In this respect, account must be taken of the state of the art, the costs of implementation, the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons.

The determination resp. decision for technical and / or organisational measures in the planning phase of the processing operations resp. in their latest development / latest review SHALL be documented and justified with regard to the principle of data protection by design (so-called decision documentation).

In this respect, within the framework of a certification procedure, the weighing up is verified by means of a document review and/or interviews. It is also checked whether processes have been implemented in the sense of a continuous audit cycle, which guarantee the consideration of the principle of data protection by design (cf. also the matrix of evaluation methods P at 1.5.1).

Relevant national law (if applicable):

N/A

1.5.2. Data protection by default

Requirement in a nutshell:

The processor SHALL take into account the principle of data protection by default. It can do so either by taking technical and organisational measures itself to ensure that, by default, only personal data whose processing is necessary for the specific purpose of the processing are processed, or by facilitating, through the design of the processing operations to be certified, the taking of such measures by controllers. It SHALL, in the sense of continuous improvement in a management system, implement processes that ensure the consideration of the principle of data protection by default both at the time of the selection resp. determination of the means (planning phase) and at the time of the actual processing. The respective processes and results shall be documented.

Concrete measures required in this respect are listed in chapter 2 of these criteria (technical and organisational measures).

Requirement in detail:

Conditions for / exceptions to the applicability of the requirement:

This requirement is always applicable. Depending on the nature of the processing operations to be certified, different measures can be considered in this respect. Therefore, the measures to be implemented must always be determined with regard to the specific target of evaluation.

Details on the subject of the requirement:

The processor SHALL design the processing operations to be certified in such a way as to ensure that by default only personal data whose processing is necessary for the specific processing purpose in question are processed. This applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, it SHALL be ensured that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.

The measures to be implemented in this respect shall be directed towards the implementation of the data protection principles of Art. 5 GDPR:

- Lawfulness;
- Fairness;
- Transparency;
- Purpose limitation;
- Data minimisation;
- Accuracy;
- Storage limitation;
- Integrity and confidentiality;
- Accountability.

Relevant national law (if applicable):

N/A

1.5.3. Provision of a data protection leaflet

This requirement is a specific requirement derived from the principles of data protection by design and by default (DPbDD).

Requirement in a nutshell:

The processor SHALL provide the controllers with a data protection leaflet which gives them a brief overview of their main data protection obligations when using the processing operations to be certified.

Requirement in detail:

Conditions for / exceptions to the applicability of the requirement:

This requirement does not apply to processing operations by processors that are used by the principals (controllers) for three or more purposes. This is because a data protection leaflet in such a case could only contain generalities and would therefore have no added value with regard to the principles of DPbDD. In such a case, it is rather sufficient if the processor provides the controllers with meaningful information on the technical and organisational measures it has implemented.

Details on the subject of the requirement:

The wording in such a data protection leaflet must be kept short and concise.[43] The threshold for individual legal advice must not be exceeded.

The leaflet SHALL contain information on the following topics, if relevant in the individual case:

1. Clarification of the roles: Certification customer = processor, principal of the certification customer = controller (always relevant),

2. Reference to specific types of processing operations and the legal framework applicable to them (if relevant),

3. Designation of the key technical and organisational measures implemented by the processor and reference to relevant documents containing more detailed information on these and other TOM (always relevant).

4. Designation of specific technical and organisational measures that the controller must implement when making use of the processing operations (if relevant),

5. Other information relevant to the data protection compliant use of the processing operations by the controller, in particular

- Designation of the services of the processor with regard to assist the controller in responding to requests for the exercise of data subject rights and with regard to compliance with the obligations of the controller pursuant to Art. 32 - 36 GDPR as well as reference to the relevant contractual clauses (always relevant),
- Preferences and related configuration options of the controller with data protection relevance (if relevant),
- Other information relevant to data protection compliant use (if relevant).

Relevant national law (if applicable):

[43] Normally, it is possible to include all relevant information in a one to two page document. The data protection experts engaged by the processor, if any, to prepare the processor for the evaluation by the certification body may assist the processor in preparing such a document.

N/A

2. Technical and organisational measures: Accompanying measures to protect the data subject

This chapter deals with **technical and organisational measures** that the processor resp. other processors engaged by the processor SHALL implement in order to ensure a level of protection appropriate to the risk to the rights and freedoms of the data subjects, rising from the processing operations to be certified (cf. Art. 32 par. 1 GDPR).

When dealing with the individual requirements of this chapter and especially when assessing the quality of the implemented technical and organisational measures, the following questions SHALL therefore always be considered:

- Are the technical and organisational measures implemented suitable for ensuring a level of protection appropriate to the identified risks to the rights and freedoms of the data subjects?
- Do the technical and organisational measures implemented support the requirements for data protection by design and by default (see chapter 1.5 of this document)?

In principle, technical measures are only appropriate if they correspond to the current state of the art. Consequently, before starting a technical evaluation, the current state of the art with regard to the technical measures implemented by the processor resp. other processors and their data protection-friendly default settings must always be determined. In this respect, EuroPriSe is guided in particular by the document "Guideline “State of the Art”" by ENISA and TeleTrust[44], to which the EDPB also refers in its “Guidelines 4/2019 on Article 25 Data Protection by Design and by Default”.[45]

However, before checking compliance with the specific requirements of this chapter resp. the appropriateness of the relevant measures, the following questions must be answered first (cf. Art. 32 par. 2 GDPR):

- What are the risks to the rights and the freedoms of the data subjects related to the intended or actual use by the controller(s) of the processing operations to be certified (in particular, accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed)?
- Can the realisation of these risks lead to physical, material or immaterial damage for the data subjects?

In answering the questions, the nature, scope, circumstances and purposes of the processing in question shall be taken into account. Risks to the rights and freedoms of the data subjects shall be assessed on the basis of an objective evaluation. As a result, it must be determined whether the processing operations in question present a risk or a high risk.

[44] https://www.teletrust.de/publikationen/broschueren/stand-der-technik/ (English version of the document available at the bottom of the page). However, corresponding statements on the state of the art in IT security must always be critically questioned with regard to the fact that the rights of the data subjects must be in the focus in the context of a data protection certification.

[45] https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42019-article-25-data-protection-design-and_en (cf. p. 8, fn. 9 + 10).

In respect of the classification of risks, the EuroPriSe methodology is based on the method of the standard data protection model of the DSK as amended from time to time.[46] Finally, on the basis of the identified risks to the rights and freedoms of the data subjects, a classification of the respective processing operations into one of the two protection requirement classes normal or high shall be made.

Technical and organisational measures may be relevant with regard to data, systems and processes that are the subject of the processing operations to be certified. If any of the following requirements are relevant to more than one of these elements, differentiation shall be made accordingly in the context of an evaluation.

The technical and organisational measures implemented by the processor resp. other processors must be considered. This also includes measures that are part of an IT component that is used to carry out the processing operations to be certified (e.g. encryption or authentication functionalities).

With regard to the principle of transparency, the documentation provided to controllers using the processing operations to be certified SHALL inform them about relevant technical and organisational measures that they themselves must implement (e.g. access control measures regarding the offices of a controller). However, this only applies if such information is of crucial importance in the specific case.

If the processor relies on other processors (sub-service providers) for the provision of its service, it SHALL be checked whether appropriate technical and organisational measures have also been contractually defined for them. This may also result in the review of contracts with further sub-service providers in terms of the TOM specified therein, depending on the criticality of the subcontracted service. The necessity of an evaluation of the technical and organisational measures in an appropriate form also for sub-service providers results from the risk assessment of the outsourced sub-processes in relation to the actual ToE.

2.1. General obligations

This chapter includes requirements that relate to general obligations such as the obligation to prevent unauthorised access to data, programmes, technical equipment / devices or systems as well as to operational sites / relevant premises, the obligation to implement measures to ensure network and transport security, the obligation to implement measures to prevent accidental loss of personal data or the obligation to ensure secure disposal and deletion of personal data.

2.1.1. Preventing unauthorised access to data, programmes, devices and premises

Requirement in a nutshell:

The processor SHALL ensure that access to premises as well as access to data, programmes and technical devices or systems is excluded for unauthorised persons. In detail, the specific (sub-)requirements 2.1.1.1 to 2.1.1.6 listed below SHALL be met.

[46] https://www.datenschutzzentrum.de/uploads/sdm/SDM-Methodology_V2.0b.pdf

2.1.1.1. Physical access control

Requirement in a nutshell:

The processor SHALL implement measures to ensure that unauthorised persons are prevented from accessing the premises and technical equipment or systems resp. that relevant other processors have implemented such measures.

Requirement in detail:

The processor SHALL demonstrate that

- the measures implemented by it resp. by relevant other processors (e.g. data centres) prevent unauthorised access to buildings, rooms, hardware, archives, mobile media, printouts etc.,
- these measures consider the existing resp. assumed risk to the rights and freedoms of the data subjects,
- measures are applied that record access by persons resp. hardware and software (traceable). Chapter 2.1.2 deals with the resulting personal data (log data).

2.1.1.2. Access to portable media and mobile devices

Requirement in a nutshell:

The processor SHALL implement measures to ensure that access to mobile (storage) media and mobile IT devices is excluded for unauthorised persons resp. that relevant other processors have implemented such measures.

Requirement in detail:

If the use of the processing operations to be certified results resp. may result in the storage of personal data on mobile media, the processor SHALL demonstrate that:

- mobile media are stored securely (e.g. in archives with restricted access),
- printouts are also stored securely,
- media and their contents are inventoried,
- the transfer of media is documented / logged.

2.1.1.3. Access to data, programmes and devices

Requirement in a nutshell:

The processor SHALL implement measures to ensure that access to data, programmes and devices by unauthorised persons is prevented, resp. that relevant other processors have implemented such measures.

Requirement in detail:

The processor SHALL demonstrate that access control mechanisms of the IT products used to provide the service are used as stipulated below. The processor SHALL have an overview at all times of the persons or roles by which access rights are managed. Furthermore, it SHALL ensure that

- devices or systems used provide access control features such as mechanical locks, PIN codes or password protection,

- SW systems offer access control functions such as a role-based authorisation concept for SAP modules,
- access rights are assigned with granularity,
- this is the case both with regard to the scope of the respective authorisations (read, modify, transmit, print, etc.) and with regard to the respective data (file, record, field, table, etc.),
- there are special roles for the administration of access rights (e.g. for granting / revoking permissions, setting up groups and roles or configuring roles for user accounts),
- the administration of access / access rights is separated (e.g. through delegation) from technical administration (e.g. creation of backups, programming activities or second-level support),
- access is controlled at each stage of processing,
- measures have been implemented to prevent unauthorised manipulation of data by users (in particular, tested measures against SQL injections),
- measures have been implemented to verify user input (in particular, tested measures to prevent XXS attacks).

2.1.1.4. Identification and authentication

Requirement in a nutshell:

The processor SHALL implement measures to ensure that individuals are identified and authenticated before they are given access to data, programmes, equipment and premises, resp. that relevant other processors have implemented such measures.

Requirement in detail:

The processor SHALL demonstrate that:

- the processing operations to be certified are secured by identification and authentication measures,
- measures have been implemented to prevent (further) repeated identification and authentication attempts after a certain number of failed attempts,
- these countermeasures (e.g. slowing down the identification process or temporarily resp. permanently deactivating user accounts) consider the existing resp. assumed risk,
- if identification and authentication is carried out using tokens (e.g. cards, keys or certificates), these are secured against replication (cloning) and unauthorised access.

2.1.1.5. Use of passwords

Requirement in a nutshell:

The processor SHALL implement measures to ensure that password protection is in place resp. that relevant other processors have implemented such measures.

Requirement in detail:

The processor SHALL demonstrate that:

- processes are implemented and effective to ensure confidential and unaltered password assignment, distribution and storage,
- a change of used passwords is required / technically enforced at regular intervals,
- passwords for the authentication of hardware or software (e.g. authentication codes for WLAN hardware or database accesses of web servers) can also be changed,
- a state of the art quality of passwords (e.g. in terms of length and complexity) is required / technically enforced,
- supporting mechanisms of the (deployed) software (e.g. the operating system) are used to control password quality and lifetime,
- precautions are provided for when a user has forgotten their password (assignment of a new password)
- a multi-factor authentication technique is used, when suitable according to the state of the art.

2.1.1.6. Organisation and documentation of access controls

Requirement in a nutshell:

The processor SHALL implement measures to ensure that access controls are in place, documented and managed resp. that relevant other processors have implemented such measures.

Requirement in detail:

The processor SHALL demonstrate that:

- the access rights are organised, clearly documented and comprehensible for each authorised user,
- the rules for the administration of access and access rights are implemented and documented,
- Access and access rights are revoked if no longer required,
- Tokens used for authentication (for example, keys, smart cards, or hardware security tokens) are also part of the inventory.

2.1.2. Logging of the processing of personal data

Requirement in a nutshell:

The processor SHALL implement measures to ensure logging of the processing of personal data resp. that relevant other processors have implemented such measures. In detail, the specific (sub-)requirements 2.1.2.1 and 2.1.2.2 listed below SHALL be met.

2.1.2.1. Logging mechanisms

Requirement in a nutshell:

The processor SHALL have implemented logging mechanisms resp. ensure that relevant other processors have implemented such mechanisms.

Requirement in detail:

The processor SHALL demonstrate that:

- with regard to the processing operations to be certified, logging mechanisms are in place to revise / supplement / rectify the personal data processed,
- this includes the possibility of tracking read, save, modify and transmit operations, as well as the possibility of recording the identity of the users who performed these actions and the time at which these actions took place,
- logging can be configured in terms of its level of detail (e.g. by limiting logging to write / insert actions) resp. it is actually configured in consideration of the existing resp. assumed risk,
- the storage duration of the log data can be configured resp. this is actually configured in consideration of the existing resp. assumed risk and the purpose of the processing,
- different types of log data (e.g. regarding the processing / transfer of personal data or the granting of access authorisations) stored in one and the same log file are stored in such a way that different storage periods (e.g. two years for access to personal data and five years for the granting of access authorisations) may apply, or these different types of log data are stored in different log files,
- the log data can be supplemented by user input (e.g. the specification of a file number to justify access to data) in a tamper-proof manner,
- a simple evaluation of the log data is possible with regard to defined questions (e.g. all changes to file XXX, all file accesses between 23:00 and 03:00 or all transmissions carried out or initiated by user YYY),
- if no automated logging functionalities are performed (resp. can be performed by the user) as part of the provision of a service, manual logging mechanisms are in place (e.g. paper-based mechanisms, "visitor book").

2.1.2.2. Operation of the logging mechanisms

Requirement in a nutshell:

The processor SHALL have implemented measures for the operation of the logging mechanisms resp. ensure that relevant other processors have implemented such measures.

Requirement in detail:

The processor SHALL demonstrate that:

- the storage period is configured to be in accordance with the relevant security policies and applicable data protection regulations,
- log data shall be reviewed regularly by the data protection officer or the IT security officer,
- log data is safely disposed of / (really) deleted after the storage period has expired,
- if logging has been blocked / deactivated, this is logged in turn.

2.1.3. Network and transport security

Requirement in a nutshell:

The processor SHALL ensure that data are transported securely and that its own networks are operated in a secure manner resp. that relevant other processors have implemented such measures. Cf. also below at “Requirement in detail:”.

Requirement in detail:

The processor SHALL demonstrate that:

- the security of remote accesses by means of which data or company networks can be accessed is comparable to that guaranteed for internal accesses (typical measures are encryption, VPN, multi-factor authentication, etc.),
- the transmission via public networks (e.g. the internet) is encrypted,
- if there is a connection between an internal and an external network, the internal network is sealed off from the external / public network (for example by firewalls),
- in the case of a firewall, the corresponding firewall rules ensure a secure separation of the networks,
- the parts of the network that are accessible both internally and externally (e.g. proxies, mail servers, etc.) are specially sealed off (for example, by a demilitarised zone - DMZ),
- the internal network is secured against malware transmitted, for example, via external connections (links) or by connecting mobile devices.

2.1.4. Mechanisms to prevent accidental loss of data; backup & recovery mechanisms

Requirement in a nutshell:

The processor SHALL ensure that mechanisms are in place to prevent accidental data loss resp. that relevant other processors have implemented such measures. In detail, the specific (sub-)requirements 2.1.4.1 to 2.1.4.4 listed below must be met.

2.1.4.1. General measures

Requirement in a nutshell:

The processor SHALL ensure that general precautionary measures against accidental data loss have been implemented and are effective.

Requirement in detail:

The processor SHALL demonstrate that:

- measures against fire, water, strong electromagnetic fields, etc. have been implemented,
- measures have been implemented against a power failure,

- an availability / redundancy concept is in place (optional or mandatory[47]),

2.1.4.2. Back-up mechanisms

Requirement in a nutshell:

The processor SHALL ensure that back-up mechanisms are effective.

Requirement in detail:

The processor SHALL demonstrate that:

- in the context of the processing by the processor, backup files are also covered by an erasure concept,
- backups are made at a frequency in accordance with any applicable legislation or internal security arrangements (if any),
- Tools are available to test the error-free functioning of the implemented backup procedures (e.g. to verify the flawlessness / readability of backup copies),
- the archiving of personal data is separated from the creation of backup copies.

2.1.4.3. Backup storage

Requirement in a nutshell:

The processor SHALL ensure that back-up copies are kept safely.

Requirement in detail:

The processor SHALL demonstrate that:

- backup files are kept / stored safely (e.g. in fire-proof safes or in other fire compartments),
- backup files are secured against unauthorised access (e.g. by encryption, especially when stored in the cloud, storage in safes).

2.1.4.4. Recovery mechanisms

Requirement in a nutshell:

The processor SHALL ensure that the recovery processes run as stipulated below at “Requirement in detail:”.

Requirement in detail:

The processor SHALL demonstrate that:

- the recovery processes have been tested,
- the recovery of individual data sets (e.g. accidentally deleted data sets) is organised (e.g. recovery only after written authorisation) and documented / logged with the help of the media used for backing up these data sets,

[47] The decision as to whether an availability / redundancy concept is optional or mandatory depends on the specific circumstances of the individual case.

- the recovery of individual data (e.g. accidentally deleted data) is organised (e.g. recovery only after written authorisation) and documented / logged with the help of the media used for backing up this data.

2.1.5. Data protection and IT security management

Requirement in a nutshell:

The processor SHALL ensure that its implemented data protection and IT security management is running as required.

2.1.5.1. Risk analysis

Requirement in a nutshell:

The processor SHALL be aware of the possible risks and threats to the rights and freedoms of the data subjects.

Requirement in detail:

The processor SHALL demonstrate that:

- a written risk analysis or, if applicable, a DPIA is available,
- this is up to date,
- covers the processing operations to be certified,
- the risk analysis / DPIA is regularly reviewed and updated,
- technical and organisational measures are selected on the basis of the risk analysis / DPIA,
- the documentation provided together with the processing operations informs about risks, possible vulnerabilities, etc., thereby facilitating the identification and implementation of security measures by the controller (chapter 1.5.3),

In respect of the classification of risks, the EuroPriSe methodology is based on the method of the standard data protection model of the DSK as amended from time to time.[48]

2.1.5.2. Documentation of technical and organisational measures for data protection

Requirement in a nutshell:

The processor SHALL have documentation of all implemented technical and organisational measures and keep it up to date. This also applies to contractually defined TOM for sub-processes outsourced to other processors.

Requirement in detail:

The processor SHALL demonstrate that:

- detailed written documentation of the technical and organisational measures is available,

[48] https://www.datenschutzzentrum.de/uploads/sdm/SDM-Methodology_V2.0b.pdf

- this is up to date,
- a version history as well as an overview of the authors and the persons responsible for implementing the measures are available.

2.1.5.3. Documentation of individual obligations

Requirement in a nutshell:

The processor SHALL ensure that all its employees and other processors acting on its behalf resp. their employees know their tasks and obligations.

Requirement in detail:

The processor SHALL demonstrate that:

- the tasks and obligations of individual persons are documented,
- the corresponding documentation is up to date,
- the documentation is easily accessible to these persons at all times (e.g. online / available on the intranet).

2.1.5.4. Inventory list of hardware, software, data and media

Requirement in a nutshell:

The processor SHALL ensure that relevant hardware, software, data and media used for the processing operations are recorded in inventories. For hardware and software, the current patch level SHALL also be documented.

Requirement in detail:

The processor SHALL demonstrate that:

- a single up-to-date inventory list of all hardware, software, data and media used for the processing of personal data, or several separate, up-to-date inventory lists are available, listing all hardware and software as well as categories of personal data and media.
- the documentation provides information on the interconnection of these corporate assets (network topology, domains, etc.), taking into account both internal connections and connections to external networks.

2.1.5.5. Storage media management

Requirement in a nutshell:

The processor SHALL ensure the controlled handling of storage media.

Requirement in detail:

The processor SHALL demonstrate that:

- media on which personal data is stored enable the identification of the information stored on them,
- these media are catalogued and stored in a place to which only those staff members have access who are authorised to do so according to the security policy,

- there is a media entry register that contains - directly or indirectly - information on the type of media in question, its serial number and the type of information stored on it,
- the media entry register also contains information on the date and time of receipt, the sender, the mode of dispatch and the person responsible for receipt (i.e. the person who acknowledged receipt) if media have been delivered,
- the media entry register also contains information on the date and time of creation, on the person who created the respective medium (i.e. the person who entered the data or copied it onto the medium) and on the person who added the medium to the register, if media have been created internally within the organisation,
- there is a media exit register containing - directly or indirectly - information on the type of media sent, its serial number, the type of information stored on it, the date and time of sending, the recipient, the method of sending and the person responsible for receiving the media.

2.1.5.6. Instruction of employees; duty of confidentiality

Requirement in a nutshell:

The processor SHALL ensure that employees are trained in their tasks and obligations as well as related data protection aspects and are subject to confidentiality obligations.

Requirement in detail:

The processor SHALL demonstrate that:

- new employees are instructed / trained with regard to their tasks and duties,
- employees are instructed and trained again at regular intervals (e.g. once a year), whereby this can be done in different ways (classroom training, self-study, etc.),
- the date, time and participants of these briefing / training events must be documented (i.e. there must be a list of the persons who participated in the respective event),
- the tasks and duties of the employees are recorded in writing,
- a breach of these tasks and duties has consequences under labour law, and this must be made clear to employees (e.g. in the employment contract or an annex to it).

2.1.5.7. Data protection and security audits

Requirement in a nutshell:

The processor / other processor SHALL ensure the consistent effectiveness of the technical and organisational data protection measures.

Requirement in detail:

The processor SHALL demonstrate that:

- data protection measures / security of processing operations are regularly reviewed,
- written records (reports) of the circumstances (date, place, names of auditors) and the results of such audits are available.

2.1.5.8. Incident management by processors

Requirement in a nutshell:

The processor SHALL ensure through a process, which may also involve other processors, to be able to respond to security or data protection incidents as well as to identified vulnerabilities. This includes processes within the scope of patch / change management.

Requirement in detail:

The processor SHALL demonstrate that:

- written procedures are in place describing the relevant actions and procedures to be taken resp. followed in the event of an incident, clearly identifying the responsible staff members and their respective roles, etc.,
- these procedures specify measures to ensure that the processor notifies the controller without undue delay after becoming aware of a personal data breach (cf. Art. 33 par. 2 GDPR),
- the assistance provided by the processor to the controller in the compliance with the obligations referred to in Art. 33 f. GDPR is part of these procedures (cf. in this respect Art. 28 par. 3 sentence 2 lit. f) GDPR),
- records of incidents that have already occurred identify the subject matter / circumstances of the incident and the remedial resp. restorative action taken,
- information about security vulnerabilities is collected (e.g. via the respective manufacturer, CERT messages, etc.) and forwarded to relevant persons / departments in the organisation (e.g. a change management team).

2.1.5.9. Test and release

Requirement in a nutshell:

The processor SHALL test and approve (new) processing operations.

Requirement in detail:

The processor SHALL demonstrate that:

- there is a formal procedure for the release of procedures and software,
- tests are planned and carried out before release,
- (exclusively) test data (e.g. anonymous data, dummy data, etc.) are used,
- test and release decisions are documented,
- functionalities are available for secure deletion of test data (including log data) after tests have been completed.

2.1.6. Disposal and erasure of personal data

Requirement in a nutshell:

The processor SHALL ensure the secure disposal and erasure of personal data. This also applies to the extent that other processors are involved.

Requirement in detail:

The processor SHALL demonstrate that:

- both complete data sets and individual data elements can be deleted,

- such deletion can be documented (for example, in a log file) in such a way that the deleted data itself is not disclosed,
- the processing operations provide functionalities for automated deletion after the expiry of certain (fixed, relative or conditional) time limits (e.g. functionalities relying on a timer or a reminder function),
- the processing operations erase data in such a way that it cannot be recovered (e.g. by overwriting data (several times) on a hard disk, CD-RW, etc.),
- the deletion method used is reliable and effective,
- if necessary, parts of the hardware used have been removed resp. "cleaned" before disposal or reuse (examples include the removal of hard drives from computers or the removal of flash memory from routers),
- if data carriers are physically destroyed (e.g. for the purpose of disposing documents, media, CD-ROMs, smart cards or tokens), the method used for this purpose is reliable and effective,
- where third party equipment is used to process personal data (e.g. leased photocopiers and the hard drives they contain), measures have been implemented to ensure that no personal data remains on this equipment when it is returned / repossessed by its owners,
- media are professionally "cleaned" resp. destroyed before their disposal,
- if the services of third-party providers are used for this purpose, this is legally permissible and only certified specialist disposal companies are used.
- the methods used for the physical destruction (of documents, media, CD-ROMs) or for the logical destruction of data (e.g. by overwriting) are reliable and effective.

2.1.7. Temporary files

Requirement in a nutshell:

The processor SHALL ensure the secure handling of temporary files as well. This also applies to the extent that other processors are involved.

Requirement in detail:

The processor SHALL demonstrate that:

- there is an overview of where temporary files are generated everywhere by the processing operations to be certified (e.g. temporary copies of documents edited using a word processing programme),
- access to these data / copies is controlled as part of the processing operations (e.g. through file shares that only apply to the users of the (original) document currently being processed),
- temporary files or data are deleted automatically,
- this is done in a secure manner (see chapter 2.1.6),
- an automated procedure is available that issues a warning if (some) temporary files could not be deleted / removed and that (subsequently) enables reliable deletion.

2.1.8. Documentation of the processing operations from the customer's point of view

Requirement in a nutshell:

The processor SHALL describe the processing operations in such a way that a customer (controller) can use them in compliance with EU data protection law.

Requirement in detail:

The processor SHALL demonstrate that:

- it provides its customers (controllers) in the form of documentation (including the data protection leaflet, see chapter 1.5.3) with all information as well as hints and recommendations for action that the customers need to fulfil their legal obligations (e.g. information on technical and organisational measures, the processor's security concept, information on (other) processors, in particular those from third countries),
- the documentation is easy to understand and use for both administrative staff (admins) and users,
- the documentation contains information, guidance and recommendations on how to use the processing operations.

2.2. Technology-specific requirements

This subchapter contains technology-specific requirements that address the topics of encryption, pseudonymisation and anonymisation.

2.2.1. Encryption

Requirement in a nutshell:

The processor SHALL use secure encryption techniques. This SHALL also be ensured with regard to other processors.

Requirement in detail:

The processor SHALL demonstrate that:

- encryption mechanisms are used for the transport of data by means of media or over insecure networks,
- encryption mechanisms are used in access control (e.g. with regard to access to databases or backup copies),
- the encryption is effective, e.g. with regard to the key lengths and algorithms used (in particular, these SHALL be renowned / proven algorithms for which no vulnerabilities have become known so far),
- the keys used are handled securely, also in case of loss or forgetting,
- the keys are transmitted in a secure manner (e.g. keys for encryption of hard disks of hosted servers).

2.2.2. Pseudonymisation and anonymisation

Requirement in a nutshell:

In principle, the processor is required to design the processing operations in such a way that compliance with the principle of data protection by design and by default is made as easy as possible for the controllers (cf. chapter 1.5 of these criteria). If it makes use of the instruments of pseudonymisation and/or anonymisation in this context, it SHALL use effective methods in this respect. This SHALL also be ensured with regard to other processors.

Requirement in detail:

N/A

3. Rights of the data subjects

Due to the particular importance of data subjects' rights, this aspect is addressed in this separate chapter of the criteria. The certification customer SHALL assist controllers in complying with their obligation to respond to requests for the exercise of applicable data subjects' rights laid down in chapter III of the GDPR. For this purpose, it SHALL implement technical and organisational measures.

While in some constellations the assistance may simply consist in forwarding any request received without delay and/or enabling the controller to directly extract and manage the relevant personal data, in certain circumstances more specific, technical tasks may be assigned to the processor. This is particularly the case if the processor is able to extract and manage the personal data.

In this respect, it must be taken into account to what extent the controller is actually dependent on the processor for the assistance of the processor regarding data subject rights. It must also be taken into account that some of the data subject rights addressed in the various sub-sections below will always be applicable, whereas others will depend on a further legal assessment of the situation or a substantial appreciation.

When dealing with this chapter, it must be checked whether the processor has implemented technical and organisational measures with regard to the support obligations towards the controller(s) provided for in the contracts with the individual controller(s) or in the contract template[49] used by the processor.

3.1. Right to information

Requirement in a nutshell:

The processor SHALL support the controllers in complying with their information obligations towards the data subjects by providing them with relevant information on the processing activities to be certified and by implementing any other technical and organisational measures provided for in this respect in the contracts with the individual controller(s) or in the contract template used by the processor.

Requirement in detail:

Prior to the start of its activities, the processor SHALL provide the controllers with the following information, which is relevant with regard to the controllers' information obligations towards the data subjects:

- Any recipients or categories of recipients to which the processor may disclose personal data when processing them on behalf of the controller (namely: any sub-processors used by the processor),
- Where applicable, the fact that the processor transfers personal data to a third country or international organisation and the appropriate or suitable safeguards in place.

Furthermore, it SHALL ensure through technical and organisational measures that the controllers are informed without delay of any changes to the processing operations to be

[49] Cf. chapter 1.2.1 of these criteria.

certified which are relevant with regard to the information obligations of the controllers towards the data subjects. This concerns e.g. the case that the processor wants to make changes that result in personal data being transferred to (further) third countries.

Relevant national law (if applicable):

N/A

3.2. Right of access

Requirement in a nutshell:

As applicable under the relevant contractual clauses (cf. section 1.2.1 2.e), the processor SHALL support the controllers in complying with their obligation to respond to requests from data subjects to exercise the right of access by

- promptly forwarding any request received,
- enabling controllers to extract all personal data relevant to respond to the request for access, and/or
- implementing any other technical and organisational measures provided for in this respect in the contracts with the individual controller(s) or in the contract template used by the processor.

Requirement in detail:

The processor SHALL support controllers in complying with their obligation to respond to requests from data subjects to exercise the right of access by implementing technical and organisational measures. In this respect, the processor SHALL at least ensure that requests from data subjects which it has received itself are forwarded to the controller without delay. If the contracts with the individual controller(s) or the contract template used by the processor provide for further support services, it SHALL also have implemented technical and organisational measures with regard to this.

Relevant national law (if applicable):

N/A

3.3. Right to rectification

Requirement in a nutshell:

As applicable under the relevant contractual clauses (cf. section 1.2.1 2.e), the processor SHALL support the controllers in complying with their obligation to respond to requests from data subjects to exercise the right to rectification by

- promptly forwarding any request received,
- enabling controllers to extract and rectify the personal data concerned, and/or
- implementing any other technical and organisational measures provided for in this respect in the contracts with the individual controller(s) or in the contract template used by the processor.

Requirement in detail:

The processor SHALL support controllers in complying with their obligation to respond to requests from data subjects to exercise the right of rectification by implementing technical and organisational measures. In this respect, the processor SHALL at least ensure that

requests from data subjects which it has received itself are forwarded to the controller without delay. If the contracts with the individual controller(s) or the contract template used by the processor provide for further support services, it SHALL also have implemented technical and organisational measures with regard to this.

Relevant national law (if applicable):

N/A

3.4. Right to erasure

Requirement in a nutshell:

As applicable under the relevant contractual clauses (cf. section 1.2.1 2.e), the processor SHALL support the controllers in complying with their obligation to respond to requests from data subjects to exercise the right to erasure by

- promptly forwarding any request received,
- enabling controllers to extract and erase the personal data concerned, and/or
- implementing any other technical and organisational measures provided for in this respect in the contracts with the individual controller(s) or in the contract template used by the processor.

Requirement in detail:

The processor SHALL support controllers in complying with their obligation to respond to requests from data subjects to exercise the right to erasure by implementing technical and organisational measures. In this respect, the processor SHALL at least ensure that requests from data subjects which it has received itself are forwarded to the controller without delay. If the contracts with the individual controller(s) or the contract template used by the processor provide for further support services, it SHALL also have implemented technical and organisational measures with regard to this.

Relevant national law (if applicable):

N/A

3.5. Right to restriction of processing

Requirement in a nutshell:

As applicable under the relevant contractual clauses (cf. section 1.2.1 2.e), the processor SHALL support the controllers in complying with their obligation to respond to requests from data subjects to exercise the right to restriction of processing by

- promptly forwarding any request received,
- enabling controllers to extract the personal data concerned and provide for restriction of processing, and/or
- implementing any other technical and organisational measures provided for in this respect in the contracts with the individual controller(s) or in the contract template used by the processor.

Requirement in detail:

The processor SHALL support controllers in complying with their obligation to respond to requests from data subjects to exercise the right to restriction of processing by implementing

technical and organisational measures. In this respect, the processor SHALL at least ensure that requests from data subjects which it has received itself are forwarded to the controller without undue delay. If the contracts with the individual controller(s) or the contract template used by the processor provide for further support services, it SHALL also have implemented technical and organisational measures with regard to this.

Relevant national law (if applicable):

N/A

3.6. Right to data portability

Requirement in a nutshell:

As applicable under the relevant contractual clauses (cf. section 1.2.1 2.e), the processor SHALL support the controllers in complying with their obligation to respond to requests from data subjects to exercise the right to data portability by

- promptly forwarding any request received,
- enabling controllers to extract the personal data in a structured, commonly used and machine-readable format and to transmit those data to another controller, and/or
- implementing any other technical and organisational measures provided for in this respect in the contracts with the individual controller(s) or in the contract template used by the processor.

Requirement in detail:

The processor SHALL support controllers in complying with their obligation to respond to requests from data subjects to exercise the right to data portability by implementing technical and organisational measures. In this respect, the processor SHALL at least ensure that requests from data subjects which it has received itself are forwarded to the controller without undue delay. If the contracts with the individual controller(s) or the contract template used by the processor provide for further support services, it SHALL also have implemented technical and organisational measures with regard to this.

Relevant national law (if applicable):

N/A

3.7. Right to object

Requirement in a nutshell:

As applicable under the relevant contractual clauses (cf. section 1.2.1 2.e), the processor SHALL support the controllers in complying with their obligation to respond to requests from data subjects to exercise the right to object by

- promptly forwarding any request received,
- enabling controllers to extract the personal data and provide for cessation of the respective processing, and/or
- implementing any other technical and organisational measures provided for in this respect in the contracts with the individual controller(s) or in the contract template used by the processor.

Requirement in detail:

The processor SHALL support controllers in complying with their obligation to respond to requests from data subjects to exercise the right to object by implementing technical and organisational measures. In this respect, the processor SHALL at least ensure that requests from data subjects which it has received itself are forwarded to the controller without delay. If the contracts with the individual controller(s) or the contract template used by the processor provide for further support services, it SHALL also have implemented technical and organisational measures with regard to this.

Relevant national law (if applicable):

N/A