European Privacy Seal

– privacy at its best

EuroPriSe Criteria Catalogue

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

v3.0

EuroPriSe Criteria Catalogue

Processing operations by processors

(v3.0 – Date of publication: Confidential draft, not yet published)

Reason(s) for change for the creation of this new version:

- Implementation of the recommendations of the European Data Protection Board (EDPB) in its Opinion 25/2022 on the criteria catalogue for processors of EuroPriSe Cert GmbH.

CONFIDENTIAL

©EuroPriSe Cert GmbH

EuroPriSe Cert GmbH

Joseph-Schumpeter-Allee 25 - D-53227 Bonn

Table of contents

CONFIDENTIAL

CONFIDENTIAL

CONFIDENTIAL

Introduction

This document contains the EuroPriSe certification criteria of a national certification scheme for Germany for the certification of processing operations by processors.[1] The subject of certifications to which this criteria catalogue applies are processing operations performed in products, processes and services or with the aid of (also several) products and services and with regard to which the certification customer is to be classified as a processor.

The scope of this criteria catalogue is not limited to certain types of processing operations. Rather, the methodology[2] underlying a EuroPriSe evaluation allows for the certification of any processing operations by processors. It is therefore a universal methodological approach on the basis of which a large number of very different processing operations can be certified. Hence, it is of fundamental importance that the methodological requirements are adhered to, as this is the only way to ensure a uniform application of the certification criteria and a comparable level of testing depth across different certification procedures. Ultimately, the aim here is to ensure maximum comparability and reproducibility of the certifications issued and their results.[3]

Processing operations by processors may be provided to only one or a few customers/principals[4]. Often, however, the processing operations will be used by a large number of customers.[5] This is one of the reasons why not only the legal obligations of the certification customer as a processor[6] matter in the context of a certification according to EuroPriSe, but also whether the processor facilitates its customers to use the processing operations to be certified in a data protection-compliant manner is always examined in the sense of a broad interpretation of the principles of data protection by design and by default[7].

[1] The requirements to be met by processing operations by controllers are not covered by this document, but are listed in a separate criteria catalogue for processing operations by controllers. Basic information on the parties involved in a certification procedure and binding rules on the course of such a procedure can be found in the rules of procedure for the certification of processing operations by controllers and processors, currently available in version 2.1.

[2] The methodological requirements, which are requirements for conformity assessment activities, are addressed in a separate document. This compendium of evaluation methodology for the certification of processing operations by processors (in short: methodology compendium P) is currently available in version 2.1. It is supplemented by the document "EuroPriSe matrix on evaluation types and methods according to ISO/IEC 17067 subs. 6.5.1 lit. b) and g)" (in short: matrix of evaluation methods P). This document is also currently available in version 2.1.

[3] This poses a particular challenge in the context of European data protection law since the interpretation of vague legal terms (e.g. "appropriate technical and organisational measures") and the balancing of interests play an important role.

[4] As a rule, these will be controllers within the meaning of Art. 4 No. 7 GDPR.

[5] e.g., SaaS services for the storage resp. exchange of documents and data in the - public - cloud.

[6] The responsibility for compliance with the provisions of the GDPR lies with the controller (cf. Art. 5 par. 2, 24 GDPR). The processor, on the other hand, is "only" subject to specific legal obligations such as the obligation to maintain a record of processing activities (Art. 30 par. 2 GDPR), the obligation to designate a data protection officer (Art. 37 GDPR), the obligation to implement appropriate technical and organisational measures (Art. 32 GDPR) or certain obligations vis-à-vis the controller (see, for example, Art. 33 par. 2 GDPR). If the processor transfers personal data to third countries or international organisations, it must also ensure compliance with the principles laid down in chapter V of the GDPR. Finally, not only the controller, but also the processor is responsible for ensuring that there is a contract or other legal act governing the processing by the processor (Art. 28 par. 3 GDPR).

[7] See in particular chapter 1.5 of this criteria catalogue.

CONFIDENTIAL

It is important to clarify that sub-processors used by a processor applying for certification cannot be certified under the EuroPriSe certification scheme. Rather, only the processing operations performed by the processor are subject to certification.

This document lists the certification criteria for processing operations by processors. Criteria are identified as such by the headings “Requirement in a nutshell” and “Requirement in detail”.

In addition, it provides guidance on how these requirements are to be applied resp. interpreted with regard to a specific target of evaluation. In this respect, in particular relevant rulings of the European Court of Justice (ECJ) and supreme court case law at Member State level[8] as well as relevant publications of the European Data Protection Board (EDPB) and national data protection supervisory authorities[9] are listed at the level of the individual requirements. These references are not part of the certification criteria as such. Rather, they are intended only as guidance to the users of this criteria catalogue. This means that in the context of each certification procedure, an up-to-date analysis of the legal framework must be carried out and documented in the evaluation concept of the certification body's evaluation team and later in its evaluation report.[10] This is the only way to ensure that current case law and publications by data protection supervisory authorities in the currently valid version are taken into account within the scope of a certification procedure. The same applies to the determination of the state of the art at the time of a certification procedure.

Where available, each requirement is also accompanied by a list of sector-specific national legislation to be taken into account (if applicable) with regard to the requirement in question.[11]

Finally, this document also contains guidance regarding checking compliance with each individual requirement. For example, it always lists which documents are typically relevant for the legal and technical evaluation of a requirement and which evaluation methods appear to be suitable resp. indispensable with regard to a requirement. More detailed information on the latter can be found in the matrix of evaluation methods P.[12] However, the final determination of the documents to be examined and the evaluation methods to be applied must always be made with regard to the specific target of evaluation and must be documented in the evaluation concept.[13]

Guidance is always designated as such and specially highlighted in terms of presentation.

The criteria catalogue is divided into three central sets of issues: Requirements from a legal perspective, requirements from a technical-organisational perspective and rights of the data

[8] In this version of the criteria catalogue, this is limited to decisions of German supreme courts.

[9] In this version of the criteria catalogue, this is limited to publications of the German Data Protection Authorities (Länder and Bund - DSK).

[10] Detailed information on this can be found in chapter 5 of the methodology compendium P (cf. fn. 2 above).

[11] In this version of the document, the listing of sector-specific national regulations is limited to those of German law. In the end, this is also merely an aid that does not render an up-to-date analysis of the legal framework and its documentation unnecessary.

[12] Cf. fn. 2 above.

[13] Cf. in this respect chapter 3 and chapters 8-12 of the methodology compendium P.

©EuroPriSe Cert GmbH

CONFIDENTIAL

subjects. More information on this division can be found at the beginning of the next chapter of this document.

This document is primarily intended for the following addressees:

- Processors seeking EuroPriSe certification,
- data protection experts who may be commissioned by such a processor to assist it in preparing for an evaluation according to EuroPriSe,
- EuroPriSe certification body staff responsible for carrying out the legal and technical evaluation resp. for reviewing the results of such an evaluation and/or the certification decision, and
- staff of the competent supervisory authority exercising its competences with regard to certifications granted by certification bodies within the meaning of Art. 43 GDPR.

CONFIDENTIAL

EuroPriSe certification criteria for processing operations by processors

This criteria catalogue contains the certification criteria for processing operations by processors.

It is divided into three chapters:

- Chapter 1: Requirements from a legal perspective
- Chapter 2: Requirements from a technical-organisational perspective
- Chapter 3: Rights of the data subjects

The first chapter addresses the requirements to be imposed on processing operations by processors from a legal perspective. In addition to more formal requirements such as the obligation to designate a data protection officer or to maintain a record of processing activities, this chapter also deals with the legal requirements with regard to the relationship between the controller and the processor as well as the relationship between the processor and other processors (if relevant). Furthermore, requirements regarding special processing operations such as the transfer of personal data to third countries (if relevant) must also be considered in the context of a legal evaluation. This chapter also covers requirements which, in the sense of a broad interpretation of the principles of data protection by design and by default require the certification customer to implement measures, which facilitate the legally compliant use of the processing operations by its principals (i.e. the controllers).

The second chapter contains the requirements to be placed on processing operations by processors from a technical and organisational point of view. Compliance with these requirements must be verified not only with regard to the certification customer itself, but also with regard to other processors. In particular, the results of the risk analysis to be carried out in preparation for the evaluation[14] shall be taken into account.

Finally, the third chapter deals with the rights of the data subjects. The requirements listed here concern the obligation of the certification customer as a processor to assist controllers to comply with their obligation to respond to requests to exercise the data subjects' rights referred to in chapter III of the GDPR.

The key word SHALL is used below. SHALL means a strict requirement.

CONFIDENTIAL

[14] Cf. chapter 4 of the methodology compendium P.

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.

Guidance

Relevant articles of the GDPR:

Art. 30 par. 2-5 GDPR

Background:

Art. 30 GDPR obliges not only the controller and, where applicable, the representatives of controllers or processors not established in the EU, but also the processor to maintain a record of processing activities under its responsibility. This obligation to maintain a record of processing activities serves to demonstrate compliance with the GDPR (cf. recital 82 of the GDPR).

For the successful completion of a certification of processing operations according to EuroPriSe, it is sufficient if the evaluation and the subsequent review conclude that the processor maintains a record of processing activities which refers to the processing operations to be certified and has established processes for the continuous updating of this record, and in this respect all individual requirements listed below at "details" are met.[15]

End of Guidance

Requirement in detail:

Conditions for / exceptions to the applicability of the requirement:

[15] A check of whether the processor fulfils its obligation under Art. 30 par. 2 GDPR also with regard to processing operations that are not covered by the ToE does not take place in the context of such certification. This is because only certain processing operations, but not the organisation as a whole resp. its data protection management system, are within the scope of the certification.

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).[16] 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.[17]

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.

[16] 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.

[17] 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.

CONFIDENTIAL

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

Guidance

Relevant documents:

1. Record of processing activities

2. Separate documents, if applicable:
List of controllers and description of the implemented TOM.

Relevant evaluation methods:

Document review, interviews

Application/interpretation aids:

- Art. 29 WP (endorsed by the EDPB): POSITION PAPER on the derogations from the obligation to maintain records of processing activities pursuant to Article 30(5) GDPR
- DE: Kurzpapier No. 1 der DSK
- DE: Hinweise zum Verzeichnis von Verarbeitungstätigkeiten, Art. 30 DS-GVO der DSK
- DE: Muster eines Verzeichnisses von Verarbeitungstätigkeiten eines Auftragsverarbeiters der DSK

End of guidance

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”.

Guidance

Relevant articles of the GDPR:

Art. 37 ff. GDPR

Background:

Art. 37 par. 1 GDPR obliges not only the controller but also the processor to appoint a data protection officer (DPO) under certain conditions. The DPO is to assist the processor as an internal control body in monitoring compliance with the GDPR (see recital 97 of the

GDPR). Due to the opening clause on the obligation to appoint a DPO (Art. 37 par. 4 sentence 1 half sentence 2 GDPR), national law also plays a role in answering the question of whether this requirement is complied with.

End of guidance

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[18] 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[19] 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.

[18] ‘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.

[19] Cf. the previous footnote.

©EuroPriSe Cert GmbH

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;
   - 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

CONFIDENTIAL

- 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.

Guidance

Relevant documents:

1. Proof of the appointment of a data protection officer (e.g. certificate of appointment).

2. Where available: Documentation of the analysis carried out by the processor as to whether it is obliged to designate a data protection officer.

Relevant evaluation methods:

Document review, interviews

Application/interpretation aids:

- Art. 29 WP (endorsed by the EDPB): Guidelines regarding Data Protection Officers ("DPOs") (WP 243 rev. 01) (cf. chapter 2: "Designation of a DPO")
- DE: Kurzpapier No.12 der DSK

End of guidance

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.

Guidance

Relevant articles of the GDPR:

Art. 3 par. 2, Art. 4 No. 17 and Art. 27 GDPR

Background:

In addition to the controller, Art. 27 par. 1 GDPR also obliges processors that do not have an establishment in the EU to designate a representative in the EU if they offer goods or services to data subjects in the Union or if they monitor their behaviour as far as their behaviour takes place within the Union. This serves to enforce the marketplace principle and thus the application and enforcement of the GDPR in third countries. Specifically, this representative, as the contact point of the processor in the EU, is supposed on the one hand to enable data subjects to effectively exercise their rights and on the other hand enable supervisory authorities to effectively enforce their supervisory measures.

In the context of a certification according to EuroPriSe, in cases where the processor does not have an establishment in the EU/EEA, it must be checked at the beginning of the

©EuroPriSe Cert GmbH

certification procedure whether the GDPR applies at all to the processing operations to be certified. If this is not the case, certification within the meaning of Art. 42 f. GDPR cannot be considered. Otherwise, the present requirement is applicable in principle[20].

End of Guidance

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[21],
    - 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

[20] The exceptional cases listed in Art. 27 par. 2 GDPR remain unaffected (see below).

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

CONFIDENTIAL

- 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;
- 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

Guidance

Relevant documents:

Proof of the written designation of a representative and its mandate in accordance with Art. 27 par. 4 GDPR (e.g. certificate of designation).

Relevant evaluation methods:

Document review, interviews

Application/interpretation aids:

- EDPB: Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) (cf. chapter 4: "Representative of controllers or processors not established in the Union")
- DE: Kurzpapier No. 7 der DSK

End of Guidance

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”.

Guidance

Relevant articles of the GDPR:

Art. 31 GDPR

Background:

Art. 31 GDPR obliges not only the controller but also the processor and, if applicable, its representative to cooperate with the competent supervisory authority in the performance of its duties upon request. If the processor has designated a data protection officer, the DPO will be the contact person for the supervisory authority (cf. in this respect also Art. 39 par. 1 lit. d) GDPR). If, on the other hand, the processor has not designated a DPO in the absence of a legal obligation, it must designate at least one person responsible for handling requests from the competent supervisory authority.

End of guidance

©EuroPriSe Cert GmbH

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

Guidance

Relevant documents:

Work instruction or similar

Relevant evaluation methods:

Document review, interviews

CONFIDENTIAL

Application/interpretation aids:

N/A

End of guidance

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[22] (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[23] must be submitted to the certification body as proof of this.

Guidance

Relevant articles of the GDPR:

Art. 28 GDPR

Background:

Art. 28 GDPR governs the content requirements for processing by a processor on behalf of the controller. A key aspect in this respect is the requirement of a data processing agreement and the requirements to be placed on it in terms of content and form.

[22] 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.

[23] 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.

©EuroPriSe Cert GmbH

To scenario 1 (see above):

Processors usually work for a large number of customers / principals (controllers). If one wanted to check within the scope of a certification whether data processing agreements have been concluded with all customers in compliance with the requirements of Art. 28 GDPR, this would normally involve an effort that would go beyond the economic scope of a certification. Therefore, a different approach is taken here: In the sense of a broad interpretation of the principles of data protection by design and by default, certification customers are required to facilitate as much as possible the data protection-compliant use of the processing operations to be certified by their principals.

In concrete terms, this means that in order to make a data protection-compliant use as easy as possible for its customers, the processor must draw up a contract template that meets all the legal requirements of Art. 28 GDPR, which must then be verified as part of the certification procedure. Alternatively, the processor may also use standard contractual clauses (cf. Art. 28 par. 6-8 GDPR).

Within the framework of a certification procedure, the following is checked in this respect (cf. also the matrix of evaluation methods P at 1.2.1):

If an individually created contract template is used:

- Review of the content of the contract template as such;
- Exemplary check of specific contracts based on the contract template.

If standard contractual clauses are used:

- Check whether the standard contractual clauses have been adopted and no clauses in conflict with them have been included[24];
- Check whether the processor has filled in annexes / free text fields that need to be completed, e.g. describing the processing operations in question;
- Exemplary check of specific contracts based on the standard contractual clauses used.

Important: Keeping a contract template does not mean that it will always be used (unchanged) resp. even that it must be used.[25] In any case, it must always be ensured that it is the controller who decides on the purposes and essential means of the processing.[26]

[24] If this is the case, no further review of the content of the clauses as such is required.

[25] Rather, the final text of the contract will usually be negotiated between the parties. As a general rule, if the controller considers accepting contractual clauses provided by the processor, it must assess them in advance in light of Art. 28 GDPR. If it accepts the contractual clauses and uses the service, it thereby also assumes full responsibility for compliance with the GDPR. This assessment is not only made easy for it if the processor uses standard contractual clauses pursuant to Art. 28 par. 6-8 GDPR, but also if its individually drafted contract template has been the subject of a certification according to EuroPriSe, since in the context of such a certification procedure it is explicitly checked whether the contract template fulfils all requirements listed in Art. 28 GDPR.

[26] If the processor attempted to use the contract template to dictate decisions resp. specifications to its contractual partner, in particular regarding the type and purpose(s) of the processing, which only a controller is entitled to, it would, in the event of success (conclusion of the agreement without changes), possibly be regarded as a (joint) controller itself. This would have the consequence that certification on the basis of this criteria catalogue would be impossible.

 ©EuroPriSe Cert GmbH

To scenario 2 (see above):

If, by way of exception, a certification customer only works exclusively for one or a few principals, it must be verified within the scope of a certification whether the processor has concluded a data processing agreement with each controller that meets the requirements of Art. 28 GDPR.

End of guidance

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):

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

CONFIDENTIAL

Blanket statements such as "contractual or business partners" are to be avoided. Instead, specific categories SHALL be designated[27], 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.

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

a) The processor processes the personal data only on documented instructions[28] 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[29] 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 this criteria catalogue 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.[30] The contractual clauses SHALL provide for an obligation for the processor to obtain the consent of the controller before making any substantial changes to

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

[28] 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.

[29] 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.

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

 ©EuroPriSe Cert GmbH

CONFIDENTIAL

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) 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.[31]

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;

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

©EuroPriSe Cert GmbH

- 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 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[32] and allows for and contributes to audits[33], 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)

Guidance

Relevant documents:

Data processing agreement (DPA) between the processor (certification customer) and the controllers using / commissioning the processing operations to be certified resp. a

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

[33] 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.

 ©EuroPriSe Cert GmbH

CONFIDENTIAL

corresponding contract template, which may be standard contractual clauses (filled in at the relevant points).

Work instruction (compliance with Art. 28 GDPR if the contract template is not used)

Relevant evaluation methods:

Document review, interviews

Application/interpretation aids:

- EDPB: Guidelines 07/2020 on the concepts of controller and processor in the GDPR (cf. part 2, chapter 1: "Relationship between controller and processor")
- DE: Kurzpapier No.13 der DSK

End of guidance

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”).

Guidance

Relevant articles of the GDPR:

Art. 28 GDPR

Background:

If certification were limited to the verification of the contractual agreements between a processor and the controller(s) (resp. to the corresponding contract template), but did not take into account whether the processor has implemented the measures necessary to implement the contractual obligations, it would only be of limited significance. Therefore, in the context of a certification of processing operations by processors according to EuroPriSe, it must also be checked whether the processor has taken the necessary steps to implement the obligations agreed in the contract resp. provided for in the contract template. The benchmark for this examination is represented by the respective contractual clauses, so that the requirements listed below must always be specified with regard to these. The requirements are accompanied by the requirements listed in chapter 2 of this document regarding technical-organisational measures, which, in view of Art. 32 GDPR and the protection goals of data protection, are always resp. usually relevant for processing operations of processors.

End of guidance

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:

©EuroPriSe Cert GmbH

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 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 this criteria catalogue).

4. Compliance with the conditions for engaging another processor.[34]

   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.[35]

   The activities required in this respect result from the relevant contractual clauses with the controller(s) - cf. chapter 1.2.1.2.e) above.[36]

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 this criteria catalogue.

[34] 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 this criteria catalogue.

[35] This is the addressed by chapter 3 of this criteria catalogue.

[36] 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).

CONFIDENTIAL

- 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 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[37] 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.[38]
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):

[37] 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.

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

CONFIDENTIAL

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)

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)

Guidance

Relevant documents:

1. Data processing agreement (DPA) between the processor (certification customer) and the controllers using / commissioning the processing operations to be certified resp. a corresponding contract template, which may be standard contractual clauses (filled in at the relevant points).

CONFIDENTIAL

2. Other documents relevant in this context, such as in particular:

   a) Data protection concept

   b) Description of the technical and organisational measures

   c) Relevant work instructions, process descriptions etc.

   (d) Templates for confidentiality resp. secrecy obligations of the relevant personnel of the processor

   e) Relevant documents resp. information on the topic of "other processors" (if relevant)

   f) Relevant documents resp. information on the topic of "transfer of personal data to third countries" (if relevant),

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

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

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

Relevant evaluation methods:

Document review, interviews

Application/interpretation aids:

- EDPB: Guidelines 07/2020 on the concepts of controller and processor in the GDPR (cf. part 2, chapter 1: "Relationship between controller and processor")
- DE: Kurzpapier No.13 der DSK

End of guidance

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.[39]

Guidance

Qualification of engaged service providers as other processors

[39] 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.

©EuroPriSe Cert GmbH

First, however, it must be clarified whether service providers engaged by the processor are to be classified as other processors within the meaning of Art. 28 par. 2 and 4 GDPR at all.

Other processors who process personal data on behalf of the certification customer are to be distinguished from service providers who are engaged by the processor and who merely provide services of a different kind which are bound by instructions. In this context, processing by another processor must already be considered if the sub-service provider has the possibility to access personal data when providing the service.

Particularly relevant in practice is the question of when services provided by a data centre result in it being qualified as another processor. Also highly relevant in practice is the question of whether testing resp. (remote) maintenance of IT systems is to be classified as processing by a(nother) processor. In this respect, the following applies:

a) Data centre services

If the data centre only provides infrastructural services and operational support, but the hardware is furnished by the customer (specifically: the processor) (so-called housing), the data centre does not qualify as another processor, unless the housing comprises shared network services including active network equipment to connect the hardware of the customer to the network.

If, on the other hand, hosting services are provided that go beyond housing (e.g. server hosting, web hosting or email hosting), then this constitutes processing by a(nother) processor.

b) Testing resp. (remote) maintenance of IT systems

If testing resp. (remote) maintenance of IT systems is agreed and the service provider has the possibility to process personal data, this constitutes processing by a(nother) processor. If, on the other hand, the service provider only carries out a technical inspection or maintenance of the corresponding infrastructure (electricity, cooling, heating), this is not to be considered as processing by a(nother) processor.

At this point it must be pointed out again that within the framework of a certification procedure, a concrete consideration of the individual case must always take place, taking into account all relevant details of the relevant application and interpretation aids.

Relevant documents:

ToE description resp. evaluation report

Relevant evaluation methods:

Document review, interviews

Application/interpretation aids:

- ECJ case law on joint controllership: Cases C-210/16, C-25/17 and C-40/17
- EDPB: Guidelines 07/2020 on the concepts of controller and processor in the GDPR (cf. part 1, chapters 1-4)
- DE: Kurzpapier No. 13 der DSK
  (in particular also on the subject of maintenance and remote access)

End of guidance

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”.

Guidance

Relevant articles of the GDPR:

Art. 28 par. 1 GDPR

End of guidance

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).[40] 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.

[40] 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

Guidance

Relevant documents:

1. Relevant work instructions, process descriptions etc.
2. Code of conduct and proof of its approval, if applicable
3. Documents on certification in accordance with Art. 42 GDPR, if applicable
4. Documents relating to a recognised international certification (e.g. ISO/IEC 2700 series), if applicable
5. Documents on the results of an external or internal audit, if applicable
6. Control options of the processor / contractual assurances, if applicable
7. Individual security concepts / TOM documents, if applicable
8. Other relevant documents such as an information security policy or a record of processing activities, if applicable

Relevant evaluation methods:

Document review, interviews

Application/interpretation aids:

- EDPB: Guidelines 07/2020 on the concepts of controller and processor in the GDPR (cf. part 2, subchapter 1.1: "Choice of the processor")
- DE: Kurzpapier No. 13 der DSK

End of guidance

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[41] submitted to the certification body as proof of this in each case.

[41] 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.

Guidance

Relevant articles of the GDPR:

Art. 28 GDPR

Background:

According to its wording, the GDPR requires that the same data protection obligations as set out in the contract between the controller and the processor shall be imposed on any other processor by way of a contract. However, this does not mean that identical contractual provisions must necessarily be imposed on the other processor.[42] Rather, it is appropriate to require that the data protection obligations and the technical and organisational measures to be implemented are specified with regard to the (processing) activities to be carried out by the other processor, whereby it must be ensured that the obligations imposed on the other processor are comparable in substance to those of the processor. Ultimately, it is crucial that the level of protection agreed between the controller and the processor is not lowered by the involvement of other processors.

End of guidance

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.

[42] For example, the contractual provisions agreed between the controller and the processor do not necessarily "fit" 1:1 to the relationship between the processor and a call centre or data centre subcontracted by the processor.

©EuroPriSe Cert GmbH

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[43], 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[44] 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[45] 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 this criteria catalogue 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

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

[44] 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.

[45] 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.

CONFIDENTIAL

implemented or refer to a separate document listing the TOM.[46] 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.[47]

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.

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

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

CONFIDENTIAL

Note: The choice of the processor SHALL be made in accordance with the choice made by the controller vis-à-vis the processor.[48]

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[49] and allows for and contributes to audits[50], 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)

Guidance

Relevant documents:

Data processing agreements (DPAs) between the processor (certification customer) and other processors engaged by the processor.

Relevant evaluation methods:

Document review, interviews

Application/interpretation aids:

- EDPB: Guidelines 07/2020 on the concepts of controller and processor in the GDPR (cf. part 2, chapter 1: "Relationship between controller and processor")

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

[49] 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.

[50] 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.

©EuroPriSe Cert GmbH

- DE: Kurzpapier No.13 der DSK

End of guidance

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.

Guidance

Relevant articles of the GDPR:

Art. 28 GDPR

Background:

In the relationship between the processor and the other processor, it must also be checked whether the processor has implemented effective measures to implement the contractual provisions. For example, the processor must have specified persons resp. departments who are authorised to issue instructions to the respective other processor and must have specified the form in which instructions are to be issued resp. documented in accordance with the relevant passages of the contract.

Since processors often use several other processors in practice, it would go beyond the scope of a certification to check with regard to all other processors whether they have specified all responsibilities and processes required to implement the contractual provisions and addressed them in binding work instructions. Therefore, the implementation of the contractual obligations in the sense of this chapter is only to be checked with regard to the processor itself.

However, the technical and organisational measures that the other processors have taken with regard to Art. 32 GDPR and the protection goals of data protection must be considered in the context of a certification. This is the addressed in chapter 2 of this criteria catalogue.

End of guidance

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:

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

©EuroPriSe Cert GmbH

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.[51]

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 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)

[51] 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.

CONFIDENTIAL

4. If applicable: National law relevant with regard to the lawfulness of an instruction (→ Art. 28 par. 3 sentence 3 GDPR)

Guidance

Relevant documents:

1. Data processing agreements (DPAs) between the processor (certification customer) and other processors engaged by the processor.
2. Other documents relevant in this context, such as in particular relevant work instructions, process descriptions, etc.

Relevant evaluation methods:

Document review, interviews

Application/interpretation aids:

- EDPB: Guidelines 07/2020 on the concepts of controller and processor in the GDPR (cf. part 2, chapter 1: "Relationship between controller and processor")
- DE: Kurzpapier No.13 der DSK

End of guidance

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.[52]

Guidance

Relevant articles of the GDPR:

Art. 28 par. 3 sentence 2 lit. b) as well as Art. 9 par. 2 lit. i), Art. 9 par. 2 lit. h) read in conjunction with par. 3, Art. 14 par. 5 lit. d) and Art. 90 GDPR

Background:

[52] Even if certification on the basis of this criteria catalogue (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.

Data protection law is closely related to statutory confidentiality obligations as well as to secrecy obligations resulting from professional and special official secrets. EU data protection law itself does not establish such special confidentiality or secrecy obligations, but merely refers in some provisions to professional secrecy and equivalent secrecy obligations that may arise from EU and Member State law, the latter being the de facto rule. In this respect, the GDPR pursues the goal of harmonising the provisions of European data protection law with the special confidentiality and secrecy obligations existing at the level of the Member States.

Both areas of law apply in parallel. This means that both areas of law apply independently of each other to processing with regard to which both special confidentiality resp. secrecy obligations and data protection requirements must be observed. If data processing is permissible under data protection law, but violates a special duty of confidentiality, it is impermissible overall. Such a violation can also result, among other things, from the fact that personal data which are the subject of a confidentiality obligation are disclosed to a processor who is not (or has not been) obliged to maintain confidentiality.

It follows from the above that it is necessary to consider special confidentiality / secrecy obligations that may exist with regard to processing operations by processors to be certified in the context of a certification according to EuroPriSe.

End of guidance

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:

- The contract template for a data processing agreement to be provided by the processor resp. the contracts concluded with individual controllers[53] SHALL address the specific confidentiality obligation.[54]
- 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

[53] Cf. chapter 1.2.1 of this criteria catalogue.

[54] 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.

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.[55]
- 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)[56]

Guidance

Relevant documents:

1. Data processing agreement between the processor (certification customer) and the controllers using / commissioning the processing operations to be certified resp. a corresponding contract template, which may be standard contractual clauses (filled in at the relevant points).

2. Contracts concluded by the processor with other processors to whom personal data subject to a confidentiality obligation are disclosed

3. If applicable, further documents resp. corresponding templates in which the processor resp. other processors are obliged to maintain confidentiality with regard to the relevant confidentiality obligation.

Relevant evaluation methods:

Document review, interviews

Application/interpretation aids:

- DE: Kurzpapier No. 13 der DSK (on 203 StGB)

End of guidance

[55] Cf. the previous footnote and chapter 1.3.2 of this criteria catalogue.

[56] - 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).

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 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.

Guidance

Relevant articles of the GDPR:

Art. 44 ff. GDPR

Background:

A transfer of personal data to third countries will occur in the context of processing operations by processors to be certified in particular if the processor relies on the services of other processors located outside the EU / EEA and thus in a third country within the meaning of Art. 44 ff. GDPR. Not least in the context of cloud computing, several such transfers resp. onward transfers can often be observed, as in many cases other processors located in third countries (e.g. operators of data centres or companies providing support and/or remote maintenance services) are involved.

However, a transfer of personal data to third countries may also occur if the processor is established within the EU resp. the EEA, the processing operations to be certified are carried out in the context of the activities of this establishment and the processing operations are at least used by some controllers established outside the EU resp. the EEA, and this is also intended to be covered by the target of evaluation (ToE).[57] In such a constellation, it must be examined whether and to what extent personal data are transferred to third countries in the context of the processing operations.

Finally, a transfer to a third country may also be considered if the processor is established in a third country, the GDPR applies to the processor pursuant to Art. 3 par. 2 and a controller established in the EU resp. the EEA who uses the processing operations transfers personal data to the processor in the third country for use in the processing

[57] However, in such a case, the ToE could also be limited to processing operations provided (only) to controllers in the EU.

operations to be certified[58] or if another processor in the EU/EEA (re)transfers personal data to the processor in the third country.

End of guidance

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[59],
2. Binding corporate rules pursuant to Art. 46 par. 2 lit. b) read in conjunction with Art. 47 GDPR[60],
3. Standard data protection clauses pursuant to Art. 46 par. 2 lit c) and d) GDPR[61],

[58] For example, in the case of web analytics services, when IP addresses are transmitted untruncated to the processor in the third country.

[59] 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

[60] 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.

[61] 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

CONFIDENTIAL

4. Approved codes of conduct pursuant to Art. 40 GDPR[62],
5. An approved certification mechanism pursuant to Art. 42 GDPR[63],
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.

Guidance
Relevant documents:

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.

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

[63] cf. the previous footnote

CONFIDENTIAL

1. Binding corporate rules and proof of their approval, if applicable

2. Standard data protection clauses used, if applicable

3. Codes of conduct and proof of their approval, if applicable

4. Documents relating to certification in accordance with Art. 42 GDPR, if applicable

5. A form for a declaration of consent, relevant contractual documents, etc. (Art. 49 GDPR), if applicable

6. Evidence with regard to supplementary measures implemented by the processor, if applicable.

Relevant evaluation methods:

Document review, interviews

Application/interpretation aids:

- ECJ: Schrems II (C-311/18)
- EDPB (on Schrems II):
  - Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data
  - Recommendations 02/2020 on the European Essential Guarantees for surveillance measures
  - Frequently Asked Questions on the judgment of the Court of Justice of the European Union in Case C-311/18 - Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems
- EDPB (other matters):
  - Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679

    At this point, reference is made to the following statement by the EDPB on the applicability of Art. 49 GDPR: “Derogations under Article 49 are exemptions from the general principle that personal data may only be transferred to third countries if an adequate level of protection is provided for in the third country or if appropriate safeguards have been adduced and the data subjects enjoy enforceable and effective rights in order to continue to benefit from their fundamental rights and safeguards. Due to this fact and in accordance with the principles inherent in European law, the derogations must be interpreted restrictively so that the exception does not become the rule. This is also supported by the wording of the title of Article 49 which states that derogations are to be used for specific situations (“Derogations for specific situations”).”
- Art. 29 WP (endorsed by the EDPB): Various documents on the subject of Binding Corporate Rules[64]

[64] WP 256 rev.01, 257 rev.01, 263 rev.01, 264 and 265 on BCR refer to the legal situation under the GDPR (cf. Art. 47) and have all been endorsed by the EDPB.

- DE: Kurzpapier No. 4 der DSK

Use Cases:

This document provides additional application aids for requirement 2.4.2 above by means of several use cases listed below.[65] The use cases address transfers of personal data to the third countries X, Y and Z and are based on the use cases 1, 2 and 6 described by the EDPB in their recommendations 01/2020. The information provided focuses on steps 3 and 4 from the series of steps suggested by the EDPB in said recommendations.

Use Case 1: End-to-end encrypted storage of personal data in a cloud hosted by a provider located in X

Facts of the case / Relevant third country transfers:

A processor (data exporter) who is based in the EU[66] provides customers (controllers) with the possibility to store personal data in a public cloud operated by a provider based in X (data importer)[67]. The storage service may be used to store all types of data (including personal data in general as well as special categories of personal data). The relevant servers are located exclusively in X.

No other entities are involved in the provision of the service and no onward transfers take place. It is to be noted already here that the processor has implemented sophisticated, state of the art end-to-end encryption.

Interim result:

There is a transfer of personal data from the EU to X because the service offered by the processor involves the storage of personal data on servers that are located in X.[68]

Transfer tool:

With regard to the transfer tool, data exporter and data importer have agreed on the standard data protection clauses 2021/914/EU. No modifications have been made to the clauses as such, nor have any supplementary measures been taken that directly or indirectly contradict the clauses.

Interim result:

The relevant transfer tool in this case are standard data protection clauses pursuant to Art. 46 par. 2 lit. c) GDPR.

Effectiveness of the transfer tool:

Relevant Laws and/or Practices of the Third Country

[65] Since this criteria catalogue only concerns processing operations by processors, the use cases listed here are selected in such a way that the respective data exporters are always processors. The following explanations relate exclusively to the topic of transferring personal data to third countries. Other legal data protection issues that may arise from the use cases are not considered.

[66] For the sake of clarity: The data exporter is not a subsidiary of a company located in X.

[67] Specifically, the data importer provides infrastructure as a service (IaaS) services such as data storage and computing capacity.

[68] At this point, however, it must be pointed out that a transfer of personal data to X would already occur if the servers were located exclusively in the EU, but the cloud provider could access the data for maintenance or support purposes.

Next, laws / practices of the third country that may impinge on the effectiveness of the appropriate safeguards of the relevant transfer tool (here: the standard data protection clauses) in the specific case must be identified.

The main subject of the respective legal review are laws in force in the relevant third country laying down requirements to disclose personal data to public authorities or granting them access to the data. In this respect, it is expressly pointed out once again that this review must be carried out with regard to the specific transfer of personal data to the third country in question.

In the case at hand, the data importer is subject to a law regulating national security and foreign intelligence-related electronic surveillance. This law ("law A") applies to providers of electronic communications services. As a provider of infrastructure as a service (IaaS) services such as data storage and computing capacity in a public cloud, the data importer qualifies as an electronic communications service provider under the relevant national law of X[69], which is why law A is applicable here. The data importer also confirmed that they have received requests for access to data from public authorities of X in the past.

Level of data protection in the third country

It must now be examined whether the level of data protection existing in the third country is essentially equivalent to that guaranteed within the EU. This examination must once again be carried out with regard to the specific transfer of personal data to the third country in question.

For this purpose, the recommendations 02/2020 of the EDPB on the European Essential Guarantees for surveillance measures can be used. Accordingly, it must be clarified whether the relevant laws and/or practices of the third country identified in the previous step meet the requirements of the European Essential Guarantees listed below:

- Processing should be based on clear, precise and accessible rules;
- Necessity and proportionality with regard to the legitimate objectives pursued need to be demonstrated,
- An independent oversight mechanism should exist and
- Effective remedies need to be available to the individual.

In the present case, it is sufficient to note that the European Court of Justice has already ruled with regard to law A that there is no level of data protection in X that is essentially equivalent to that in the EU: "It is thus apparent that law A does not indicate any limitations on the power it confers to implement surveillance programmes for the purposes of foreign intelligence or the existence of guarantees for non-X persons potentially targeted by those programmes. In those circumstances, that article cannot ensure a level of protection essentially equivalent to that guaranteed by the Charter of Fundamental Rights of the European Union (CFR), as interpreted by the relevant case-law, according to which a legal basis which permits interference with fundamental rights must, in order to satisfy the requirements of the principle of proportionality, itself define the scope of the limitation on the exercise of the right concerned and lay down clear and precise rules governing the

[69] Providers of electronic communications services under this law include, among others, providers of remote computing services, which provide computer storage or processing services to the public by means of an electronic communications system. The data importer qualifies as provider of such a remote computing service due to the IaaS services it offers.

©EuroPriSe Cert GmbH

scope and application of the measure in question and imposing minimum safeguards." (quoted from the respective judgement of the ECJ dealing with the legal situation in X).

Interim Result

The relevant laws and/or practices of the third country X in the specific case do not satisfy the European Essential Guarantees and are thus not suitable to ensure a level of protection essentially equivalent to that guaranteed within the EU. Consequently, the standard data protection clauses are not effective and it must be verified whether effective supplementary measures have been implemented (cf. below).

Existence of Effective Supplementary Measures:

At this stage, it must be verified whether supplementary measures have been taken, which, when added to the safeguards contained in the relevant transfer tool (here: the standard data protection clauses), could ensure that the personal data transferred is afforded in the third country a level of protection essentially equivalent to that guaranteed within the EU.

In the case at hand, the processor has adopted supplementary measures of a technical nature. More precisely, they have implemented a sophisticated end-to-end encryption according to the state of the art. Apart from that, the processor has not implemented any further supplementary measures.

In respect of the implemented end-to-end encryption, the processor has ensured specifically that[70]

- Strong encryption is used prior to the transfer,
- The encryption algorithm and its parameterisation conform to the state of the art and can be considered robust,
- The strength of the encryption and key length takes into account the specific time period during which the confidentiality of the encrypted personal data must be preserved,
- The encryption algorithm is implemented correctly and by properly maintained software without known vulnerabilities,
- The keys are reliably managed, and
- The keys are retained solely under the control of the data exporter.

This means that the implemented end-to-end encryption solution meets all requirements listed by the EDPB in their recommendations 01/2020 (cf. use case 1 – margin number 84). When added to the safeguards contained in the relevant transfer tool (i.e. the standard data protection clauses), it ensures that the personal data transferred is afforded in the third country a level of protection essentially equivalent to that guaranteed within the EU.

Since the implemented end-to-end encryption solution as such (together with the standard data protection clauses) already provides for such a level of protection there is no need to

[70] List in (partially) abbreviated form compared to the EDPB's recommendations 01/2020 (cf. use case 1 - margin no. 84). As a result, however, it is assumed here that the processor fully complies with all the requirements listed in the recommendations.

adopt further supplementary measures here (in other words, a combination of several supplementary measures is not required).

Interim Result:

The processor has implemented supplementary (technical) measures that, together with the safeguards contained in the standard data protection clauses, ensure that the personal data transferred is afforded a level of protection in the third country that is essentially equivalent to that guaranteed within the EU.

Final Result:

The transfer of personal data to X is permitted in the present case.

Use Case 2: Transfer of pseudonymised health data to a specialised service provider located in Y

Facts of the case / Relevant third country transfers:

A processor (data exporter) who is based in the EU is to analyse health data for a large medical institution (controller), also located in the EU, to find certain correlations that could enable the development of new treatments. For this purpose, the processor receives personal data on more than 10,000 patients. However, certain analysis operations are not carried out by the processor themselves, but by a company specialising in this area, which is based in Y.[71] This company (data importer) belongs to a group of undertakings controlled by the processor.

No other entities are involved in the provision of the service and no onward transfers take place. It is to be noted already here that the processor pseudonymises the health data before transmitting it to the data importer.

Interim result:

There is a transfer of personal data from the EU to Y.

Transfer tool:

The processor submitted to the competent supervisory authority binding corporate rules for processors, which have been approved by the supervisory authority after going through the relevant procedure. The transfer of personal data to Y at issue here is covered by the material scope of the BCR.

Interim result:

Binding corporate rules for processors pursuant to Art. 47 of the GDPR are used as the transfer tool in this case.

Effectiveness of the transfer tool:

Relevant Laws and/or Practices of the Third Country

Next, laws / practices of the third country that may impinge on the effectiveness of the appropriate safeguards of the relevant transfer tool (here: the BCR for processors) in the specific case must be identified.

[71] The analysis operations are carried out in Y on the specialised company's own computer systems.

The main subject of the respective legal review are laws in force in the relevant third country laying down requirements to disclose personal data to public authorities or granting them access to the data. In this respect, it is expressly pointed out once again that this review must be carried out with regard to the specific transfer of personal data to the third country in question.

In the case at hand, the data importer is subject to a law (“law B”) authorising the central or state government to direct an agency of the appropriate government to intercept, monitor or decrypt any information generated, transmitted, received, or stored in any computer resource[72]. This is subject to the requirement that the directing entity is satisfied that it is necessary or expedient so to do, in the interest of the sovereignty or integrity of Y, defence of Y, the security of the state, friendly relations with foreign states or public order or for preventing incitement to the commission of any cognisable offense relating to above or for investigation of any offense. At the same time, the subscriber or intermediary or any person in-charge of the computer resource are required, at the request of one of the above-mentioned agencies, to extend all facilities and technical assistance to

(a) provide access to or secure access to the computer resource generating, transmitting, receiving or storing such information; or

(b) intercept, monitor, or decrypt the information, as the case may be; or

(c) provide information stored in the computer resource.

Provided that the requirements of law B are met, competent entities may ultimately take possession of information from any computer resource. Consequently, this provision is (potentially) relevant in the present case.

In exercise of the powers conferred on it by law B, the central government of Y has issued relevant rules (“rules C”). These include rules on who may issue wiretap and surveillance orders, how those orders are to be carried out, how long they remain in effect, and to whom data may be disclosed, as well as an obligation to consider alternative means of obtaining information. In addition, another rule states that a review committee composed of senior members of the central resp. state government ("secretaries to the government") must meet at least once every two months to review all cases of wiretapping, surveillance, and decryption.

In a judgement, the Supreme Court of Y recognised the right to privacy as an expression of the constitution of Y and thus as a fundamental right. According to the court, this right includes, among others, the right to informational privacy. The fundamental right to privacy also applies to EU citizens. In its ruling, the court recognised principles such as "lawfulness, legitimate purpose, proportionality and procedural guarantees” as binding in the context of the right to privacy. These legal rights apply to EU citizens, too.

Y does not yet have a comprehensive general data protection law.

Level of data protection in the third country

It must now be examined whether the level of data protection existing in the third country is essentially equivalent to that guaranteed within the EU. This examination must once

[72] The term computer resource here means computer, computer system, computer network, data, computer database or software.

again be carried out with regard to the specific transfer of personal data to the third country in question.

For this purpose, the recommendations 02/2020 of the EDPB on the European Essential Guarantees for surveillance measures can be used. Accordingly, it must be clarified whether the relevant laws and/or practices of the third country identified in the previous step meet the requirements of the European Essential Guarantees listed below:

- Processing should be based on clear, precise and accessible rules;
- Necessity and proportionality with regard to the legitimate objectives pursued need to be demonstrated,
- An independent oversight mechanism should exist and
- Effective remedies need to be available to the individual.

At this point, no detailed analysis of the legal situation applicable in Y can be made, as this would go beyond the scope of a criteria catalogue. However, the following must be pointed out:

Y's law lacks an explicit definition of the categories of people who can be surveilled. However, such a requirement is necessary according to the case law of the European Court of Human Rights (ECtHR).[73] Thus, it is doubtful whether the processing is based on clear, precise and accessible rules.

The review committees presented above are composed of senior members of the central resp. state government ("secretaries to the government"). Therefore, it is doubtful that this is an independent oversight mechanism.

It must also be pointed out once again that there is no general, comprehensive data protection law in Y to date. Currently, there is no independent data protection supervisory authority in Y either.

Interim result:

There are significant doubts that the relevant laws and/or practices of the third country Y in the specific case satisfy the European Essential Guarantees and that they are suitable to ensure a level of protection essentially equivalent to that guaranteed within the EU. Consequently, it is assumed in the present case that the binding corporate rules for processors are not effective, which is why it must be verified whether effective supplementary measures have been implemented (see below).

Existence of Effective Supplementary Measures:

At this stage, it must be verified whether supplementary measures have been taken, which, when added to the safeguards contained in the relevant transfer tool (here: the BCR for processors), could ensure that the personal data transferred is afforded in the third country a level of protection essentially equivalent to that guaranteed within the EU.

In the present case, the processor has implemented supplementary technical measures consisting of pseudonymising the health data prior to their transfer to Y. In doing so, they replace patient names with randomly generated identification numbers ("identifiers") and

[73] EGMR, 29. Juni 2006, Weber und Saravia (54934/00), margin number 95. See also the EDPB's recommendations 01/2020, margin number 30.

information on age, height and weight with information on membership of a specific group ("clusters" - e.g. age: 20-29 years or weight: 70-79 kg). The groups are selected in such a way that the data as such (even in an overall view of all available information) can no longer be assigned to a specific data subject. Not least, no information is stored on diseases and their circumstances that are so unique that it would be within the realm of possibility to use them to draw conclusions about the identity of individual patients. Finally, the data does not concern the use of information services.[74]

The processor stores the additional information by means of which the pseudonymised data can be (re)assigned to a specific person in a dedicated, state of the art secured database located on servers within the EU, over which it has sole control.[75]

The processor has not implemented any further supplementary measures beyond pseudonymisation.

It follows from the above that the processor has ensured the following with respect to the implemented pseudonymisation:[76]

- They transfer the personal data in such a manner that it can no longer be attributed to a specific data subject without the use of additional information,
- the additional information is held exclusively by them and kept separately in an EU Member State,
- the disclosure or unauthorised use of that additional information is prevented by appropriate technical and organisational safeguards, it is ensured that the processor retains sole control of the algorithm or repository that enables re-identification using the additional information,
- they have established by means of a thorough analysis of the data in question – taking into account any information that the public authorities of the recipient country may be expected to possess and use – that the pseudonymised personal data cannot be attributed to an identified or identifiable natural person even if cross-referenced with such information.

This means that the implemented pseudonymisation meets all requirements listed by the EDPB in their recommendations 01/2020 (cf. use case 2 – margin number 85).[77] When added to the safeguards contained in the relevant transfer tool (i.e. the binding corporate

[74] For this, see use case 2 – margin numbers 86 ff. of the EDPB's recommendations 01/2020.

[75] Even if the data importer belongs to the same group of undertakings as the processor, they do not have technical permissions to access this database. On the part of the processor, there is a work instruction directing employees not to allow employees of other companies in the group to access this database under any circumstances, respectively to pass on or otherwise disclose the additional information stored in the database to them.

[76] List in (partially) abbreviated form compared to the EDPB's recommendations 01/2020 (cf. use case 2 - margin no. 85). As a result, however, it is to be assumed here that the processor fully complies with all the requirements listed in the recommendations.

[77] It must be noted that the subscriber or intermediary or any person in-charge of the computer resource are required under law B, at the request of one of the competent agencies, to extend all facilities and technical assistance to decrypt encrypted information. According to rules C, "decryption" means the process of conversion of information in non-intelligible form to an intelligible form via a mathematical formula, code, password or algorithm or a combination thereof. Whether this legal definition also includes the disclosure of additional information pursuant to Art. 4 No. 5 GDPR can be left open, since in the present case the processor has sole control over this information resp. the corresponding database.

rules for processors), it ensures that the personal data transferred is afforded in the third country a level of protection essentially equivalent to that guaranteed within the EU.

Since the implemented pseudonymisation solution as such (together with the BCR for processors) already provides for such a level of protection there is no need to adopt further supplementary measures here (in other words, a combination of several supplementary measures is not required).

Interim result:

The processor has implemented supplementary (technical) measures that, together with the safeguards contained in the standard data protection clauses, ensure that the personal data transferred is afforded a level of protection in the third country that is essentially equivalent to that guaranteed within the EU.

Final Result:

The transfer of personal data to Y is permitted in the present case.

Use Case 3: Transfer of consumer data to a call centre located in Z

Facts of the case / Relevant third country transfers:

An EU-based call centre (processor / data exporter) provides customer service, complaint management, and market research services to the provider of an online shop (controller) also located in the EU. For this purpose, the processor can access personal data[78] of more than 100,000 consumers stored on servers in the EU.[79] When providing the services, the processor has another call centre (data importer), which is based in Z, assist it as needed (e.g., during peak workloads). For this purpose, the data importer also gains access to (potentially) all personal data in plain text.

No other entities are involved in the provision of the service and no onward transfers take place.

Interim result:

The data importer accesses consumers' personal data remotely, and therefore there is a transfer of personal data from the EU to Z.[80]

Transfer tool:

With regard to the transfer tool, data exporter and data importer have agreed on standard data protection clauses adopted by a supervisory authority and approved by the European Commission pursuant to the examination procedure referred to in Art. 93 par. 2 GDPR. No modifications have been made to the clauses as such, nor have any supplementary measures been taken that directly or indirectly contradict the clauses.

Interim result:

[78] These are name, address, other contact data, demographic data and contract data.

[79] When processing this personal data, the call centre (processor) has no significant decision-making scope of its own.

[80] Cf. margin number 13 of the EDPB's recommendations 01/2020.

©EuroPriSe Cert GmbH

The relevant transfer tool in this case are standard data protection clauses pursuant to Art. 46 par. 2 lit. d) GDPR.

Effectiveness of the transfer tool:

Relevant Laws and/or Practices of the Third Country

Next, laws / practices of the third country that may impinge on the effectiveness of the appropriate safeguards of the relevant transfer tool (here: the standard data protection clauses) in the specific case must be identified.

The main subject of the respective legal review are laws in force in the relevant third country laying down requirements to disclose personal data to public authorities or granting them access to the data. In this respect, it is expressly pointed out once again that this review must be carried out with regard to the specific transfer of personal data to the third country in question.

In the case at hand, the data importer is subject to a law ("law D") governing the interception of communications both in the framework of criminal proceedings and outside such framework, in particular in connection with "events or activities endangering national, military, economic or ecological security".[81] For the purposes of this use case, the focus of consideration is on the latter.

Operational-search activities pursuant to law D include, inter alia, the interception of postal, telegraphic, telephone and other forms of communication and the collection of data from technical channels of communication. As this use case is about a call centre, the following explanations focus on the interception of communications via telephone.[82]

The respective operational-search activities may be conducted following the receipt of information, inter alia, about events or activities endangering the national, military, economic or ecological security of Z on the basis of a court decision.

Provided that the requirements of law D are met, the administrative bodies engaged in operational-search activities may take possession of personal data obtained by means of interception of telephone conversations. Consequently, this law is (potentially) relevant in the present case.

It is worth pointing out here that the European Court of Human Rights (ECtHR) found that the legal provisions of Z governing interceptions of communications do not provide for adequate and effective guarantees against arbitrariness and the risk of abuse. In view of several shortcomings[83] it had identified, the court held that the law of Z does not meet the "quality of law" requirement and is incapable of keeping the "interference" to what is "necessary in a democratic society". For this reason, the ECtHR affirmed a violation of Art. 8 European Convention on Human Rights (ECHR).

[81] Since personal data of EU citizens are at stake here, it is to be pointed out that – according to the law D – citizenship and nationality shall not be an obstacle to launching with respect to them the operational-search measures on the territory of Z, unless otherwise stipulated by the Federal Law.

[82] It is safe to assume that during phone calls between the call centre and the consumers, personal data about the latter will be mentioned, which the respective employee will either retrieve from the servers in the EU during the conversation or collect anew and then store on the servers in the EU.

[83] These shortcomings will be introduced in detail below.

Brief overview on the legal sources of Z's data protection law:

Two articles of the Constitution of Z provide the constitutional basis for data protection.[84]

Z ratified the 1981 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108). Z signed the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Treaty 223), but has not ratified it yet.

Statutory regulations on data protection can be found in the Personal Data Law of Z.

The main regulator for data protection is the Federal Service for Supervision of Communications, Information Technology and Mass Media.

Level of data protection in the third country

It must now be examined whether the level of data protection existing in the third country is essentially equivalent to that guaranteed within the EU. This examination must once again be carried out with regard to the specific transfer of personal data to the third country in question.

For this purpose, the recommendations 02/2020 of the EDPB on the European Essential Guarantees for surveillance measures can be used. Accordingly, it must be clarified whether the relevant laws and/or practices of the third country identified in the previous step meet the requirements of the European Essential Guarantees listed below:

- Processing should be based on clear, precise and accessible rules;
- Necessity and proportionality with regard to the legitimate objectives pursued need to be demonstrated,
- An independent oversight mechanism should exist and
- Effective remedies need to be available to the individual.

At this point, no detailed analysis of the legal situation applicable in Z can be made, as this would go beyond the scope of a criteria catalogue. However, the following must be pointed out: In its judgement on the legal provisions of Z governing interceptions of communications, the ECtHR identified shortcomings in the (then) laws and practices of Z governing interceptions of communications. These shortcomings concern(ed) all European Essential Guarantees as is outlined below:

Clear, precise and accessible rules:

- The circumstances in which public authorities are empowered to resort to secret surveillance measures are not defined with sufficient clarity;

Necessity and proportionality:

- Provisions on discontinuation of secret surveillance measures do not provide sufficient guarantees against arbitrary interference;
- Domestic law permits automatic storage of clearly irrelevant data;

[84] Most relevant in respect of this use case is the following article: "Everyone shall have the right to privacy of correspondence, of telephone conversations and of postal, telegraph and other communications. This right may be limited only on the basis of a court order."

Independent oversight mechanism:

- The authorisation procedures are not capable of ensuring that secret surveillance measures are ordered only when “necessary in a democratic society”;
- The supervision of interceptions does not comply with the requirements of independence, powers and competence which are sufficient to exercise an effective and continuous control, public scrutiny and effectiveness in practice*;*

Effective remedies:

- The effectiveness of the remedies is undermined by the absence of notification at any point of interceptions, or adequate access to documents relating to interceptions.

From the above it is clear that Z’s laws and practices did not meet the Essential European Guarantees at the time of the ECtHR’s judgment. Since then, laws and practices have not changed to the better in these respects. Rather, new laws have been introduced that grant even more powers to the intelligence agencies and provide for extensive storage obligations for providers of telecommunication services. In particular, several laws on the Counteraction of Terrorism are to be mentioned here:

Amongst others, the respective legal amendments require telecom providers to store text messages, voice information, images, sounds, video and other messages of communication services users (content data) for 6 months, and the metadata on them for 3 years. Telecom companies are required to disclose these content and metadata as well as "other information necessary" to the competent authorities on request and without a court order.

It must also be pointed out that Z’s main regulator for data protection is not only competent for data protection supervision, but also for various other matters (including censoring Z’s mass media), and that it reports to the Ministry of Digital Development, Communications and Mass Media. Hence, it is at least questionable if this regulator acts independently when performing their tasks as a data protection supervisory authority.

Interim result:

There are significant doubts that the relevant laws and/or practices of the third country Z in the specific case satisfy the European Essential Guarantees and that they are suitable to ensure a level of protection essentially equivalent to that guaranteed within the EU. Consequently, it is assumed in the present case that the standard data protection clauses are not effective, which is why it must be verified whether effective supplementary measures have been implemented (see below).

Existence of Effective Supplementary Measures:

At this stage, it must be verified whether supplementary measures have been taken, which, when added to the safeguards contained in the relevant transfer tool (here: the standard data protection clauses), could ensure that the personal data transferred is afforded in the third country a level of protection essentially equivalent to that guaranteed within the EU.

According to the EDPB, there will be situations where only appropriately implemented technical measures might impede or render ineffective access by public authorities in third

countries to personal data, in particular for surveillance purposes.[85] The use case at hand is such a case. It is therefore necessary to check whether the processor has implemented effective technical supplementary measures.

The personal data at stake is neither encrypted nor pseudonymised in line with the respective requirements of the EDPB.[86] Rather, the data importer has access to the personal data in the clear and there are no effective technical measures in place to prevent the interception of phone calls between the data importer and consumers. Therefore, no effective technical supplementary measures are in place.[87]

Interim result:

The processor has not implemented supplementary (technical) measures that, together with the safeguards contained in the standard data protection clauses, ensure that the personal data transferred is afforded a level of protection in the third country that is essentially equivalent to that guaranteed within the EU.

Final Result:

The transfer of personal data to Z is not permitted in the present case.

End of guidance

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.

Guidance

Relevant articles of the GDPR:

Art. 28 par. 3 sentence 2 lit. a) GDPR

Background:

A data processing agreement must stipulate, among other things, that the processor processes the personal data only on documented instructions from the controller.[88] According to Art. 28 par. 4 sentence 1 GDPR, the same also applies to contracts between a processor and other processors. In this context, it SHALL also be determined whether processing may take place in a third country outside the Union or by an international organisation.

End of guidance

[85] See margin number 53 of the EDPB's recommendations 01/2020.

[86] See use case 1 (margin number 84) and use case 2 (margin numbers 85 ff.) of the EDPB's recommendations 01/2020.

[87] This results from margin number 93 and use case 6 (margin numbers 94 ff.) of the EDPB's recommendations 01/2020.

[88] The only exception is if the processor is obliged by EU or Member State law to carry out a specific processing operation.

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

Guidance

Relevant documents:

1. Data processing agreement between the processor (certification customer) and the controllers using / commissioning the processing operations to be certified resp. a corresponding contract template, which may be standard contractual clauses (filled in at the relevant points).

2. Contracts concluded by the processor with other processors

Relevant evaluation methods:

Document review, interviews

Application/interpretation aids:

N/A

End of guidance

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.[89] 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.

[89] See also recital 78 of the GDPR.

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) 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 this criteria catalogue (technical and organisational measures).

Guidance

Relevant articles of the GDPR:

Art. 25 par. 1 read in conjunction with Art. 5 GDPR

End of guidance

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.

CONFIDENTIAL

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

Guidance

Relevant documents:

- ToE description (MUST)
- "TOM document" - description of the implemented technical and organisational measures (MUST)
- Decision documentation, if applicable
- Data protection leaflet, if applicable

Relevant evaluation methods:

Document review, interviews

Application/interpretation aids:

- EDPB: Guidelines 4/2019 on Article 25 Data Protection by Design and by Default (cf. in particular chapters 2.1 and 3)

End of guidance

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 this criteria catalogue (technical and organisational measures).

Guidance

©EuroPriSe Cert GmbH

Relevant articles of the GDPR:

Art. 25 par. 2 read in conjunction with Art. 5 GDPR

End of guidance

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

Guidance

Relevant documents:

- ToE description (MUST)
- "TOM document" - description of the implemented technical and organisational measures (MUST)
- Data protection leaflet, if applicable

Relevant evaluation methods:

CONFIDENTIAL

Document review, interviews, check of a standard configuration, identification of possible options for making personal data accessible to an indefinite number of natural persons

Application/interpretation aids:

- EDPB: Guidelines 4/2019 on Article 25 Data Protection by Design and by Default (cf. in particular chapters 2.2 and 3)

End of guidance

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.

Guidance

Relevant articles of the GDPR:

Art. 25 GDPR read in conjunction with. Art. 5 GDPR

Background:

The controller is responsible for the lawfulness of the processing. However, the processor may design the processing operations to be certified with regard to the principles of DPbDD in such a way that they make it easy for the controllers to implement the data protection principles of Art. 5 GDPR.

In practice, processors often provide very specific processing operations which may be subject to sector-specific legislation at EU resp. Member State level. In many cases, such specialised processors develop a higher level of expertise (also with regard to the legal framework) than that typically initially available to a controller. In such a case, the implementation of the data protection principles of Art. 5 GDPR is facilitated for the controller if it is provided in advance with a leaflet listing the most important legal and technical/organisational framework conditions to be observed when using the processing operations.

End of guidance

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:

©EuroPriSe Cert GmbH

The wording in such a data protection leaflet must be kept short and concise.[90] 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):

N/A

Guidance

Relevant documents:

Data protection leaflet

Relevant evaluation methods:

Document review, interviews

Application/interpretation aids:

N/A, as the documents that can be considered in this respect cannot be narrowed down in a meaningful way.

End of guidance

[90] 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.

©EuroPriSe Cert GmbH

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[91], to which the EDPB also refers in its “Guidelines 4/2019 on Article 25 Data Protection by Design and by Default”.[92]

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)[93]:

- 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

[91] 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.

[92] 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).

[93] Cf. chapter 4 of the Methodology Compendium P.

CONFIDENTIAL

be determined whether the processing operations in question present a risk or a high risk. 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.[94] 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.

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

CONFIDENTIAL

Guidance

Relevant articles of the GDPR:

Art. 5 par. 1 lit. f) and Art. 32 par. 1 lit. b) GDPR

Introduction / Overview:

Preventing unauthorised access to data etc. is one of the key measures to prevent loss of integrity, confidentiality and availability of personal data. Access to data etc. must be regulated on both a physical and a logical level: Physical access here means access to buildings and rooms as well as hardware, communication lines, data carriers, etc., whereas the term logical access refers to (non-physical) access to data, software, functions, etc. From a technical point of view, the term access is not limited to access by natural persons, but also includes access by hardware (e.g. access control of network components such as routers) and software (e.g. access of database drivers to databases).

End of guidance

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.

Guidance

Relevant articles of the GDPR:

Art. 5 par. 1 lit. f) and Art. 32 par. 1 lit. b) GDPR

Introduction / Overview:

Physical access control concerns the actual ("real life") processing of personal data. Consequently, all processing operations as well as the relevant sites/premises must be evaluated with regard to the implementation of physical access control measures.

End of guidance

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).

Guidance

Evaluation methods:

Typically, the following evaluation methods are to be used:

- On-site audit to monitor effectiveness
- Interviews with supervisors and employees
- Document review
- Consideration of relevant other certifications

Documents:

Typically, the following documents are relevant in this respect:

- Relevant third-party certifications with associated test reports
- Risk analysis of the (other) processor
- Process descriptions
- Relevant policies and regulations
- Training materials for employees

Testing tools / application aids:

The relevant test modules of the German BSI[95] can be used as a guideline for checks. These both reflect the state of the art and differentiate between measures according to risk classes. In addition, ENISA offers relevant support and, together with TeleTrusT, provides a practical guide to the state of the art[96].

End of guidance

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.

Guidance

Relevant articles of the GDPR:

Art. 5 par. 1 lit. f) and Art. 32 par. 1 lit. b) GDPR

Introduction / Overview:

Controlling (physical) access to mobile media on which personal data is stored (CDs/DVDs, USB sticks, external hard drives, tapes, etc.) is crucial because logical

[95] In the "Publications" section, most of the relevant technical guidelines and standards are offered and continuously updated: https://www.bsi.bund.de/EN/Service-Navi/Publications/publications_node.html

[96] In this respect, EuroPriSe is guided in particular by the following document from ENISA and TeleTrust: Handreichung Stand der Technik in der IT-Sicherheit (https://www.teletrust.de/publikationen/broschueren/stand-der-technik/ - English version of the document available at the bottom of the page). Corresponding statements on the state of the art in IT security must always be critically questioned in view of the fact that the rights of the data subjects must be paramount in the context of a data protection certification.

access controls such as read and write permissions related to files or database tables can often be (easily) circumvented once the attacker has access to these media. The same applies to mobile devices (laptops, tablets, smartphones, etc.) on which personal data is stored.

End of guidance

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.

Guidance

Evaluation methods:

Typically, the following evaluation methods are used:

- On-site audit to monitor effectiveness
- Interviews with supervisors and employees
- Document review
- Consideration of relevant other certifications

Documents:

Typically, the following documents are relevant in this respect:

- Relevant third-party certifications with associated test reports
- Risk analysis of the (other) processor
- Process descriptions
- Relevant policies and regulations
- Training materials for employees

Testing tools / application aids:

The relevant test modules of the German BSI can be used as a guideline for checks. These both reflect the state of the art and differentiate between measures according to risk classes. In addition, ENISA offers relevant support and, together with TeleTrusT, provides a practical guide to the state of the art.

End of guidance

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.

Guidance

Relevant articles of the GDPR:

Art. 5 par. 1 lit. f) and Art. 32 par. 1 lit. b) GDPR

Introduction / Overview:

Access to data and programmes is often controlled by means of logical mechanisms rather than physical ones: Typical access control mechanisms are the granting of permissions for reading and writing to files or the use of software or software functionalities embedded within the operating system, database management system or an application. The granularity of the control mechanisms must be evaluated, always keeping in mind that an easy management of such a system is of importance. Furthermore, the quality of the implementation must be evaluated. This is especially true for web-based applications.

Controlling access to devices can be done either on a logical level (e.g. through BIOS passwords or through PIN codes for landline or mobile phones) or on a physical level (e.g. through electromechanical interlocks).

End of guidance

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),

CONFIDE

- measures have been implemented to verify user input (in particular, tested measures to prevent XXS attacks).

Guidance

Evaluation methods:

Typically, the following evaluation methods are used:

- On-site audit to monitor effectiveness
- Interviews with supervisors and employees
- Document review
- Consideration of relevant other certifications
- Test access / account

Documents:

Typically, the following documents are relevant in this respect:

- Relevant third-party certifications with associated test reports
- Risk analysis of the (other) processor
- Process descriptions
- Relevant policies and regulations
- Training materials for employees
- Contracts with other processors (in particular: requirements for TOM), if applicable

Testing tools / application aids:

The relevant test modules of the German BSI can be used as a guideline for checks. These both reflect the state of the art and differentiate between measures according to risk classes. In addition, ENISA offers relevant support and, together with TeleTrusT, provides a practical guide to the state of the art.

End of guidance

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.

Guidance

Relevant articles of the GDPR:

Art. 5 par. 1 lit. f) and Art. 32 par. 1 lit. b) GDPR

Introduction / Overview:

A prerequisite for the granting of access is always the successful identification and authentication of the user. The same applies to hardware and software. Typical mechanisms for this are the use of login names and passwords, biometric systems,

security tokens and cryptographic keys (certificates). Randomly generated identifiers such as session keys for web-based applications are also used for identification and authentication.

End of guidance

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.

Guidance

Evaluation methods:

Typically, the following evaluation methods are used:

- On-site audit to monitor effectiveness
- Interviews with supervisors and employees
- Document review
- Consideration of relevant other certifications
- Test access / account

Documents:

Typically, the following documents are relevant in this respect:

- Relevant third-party certifications with associated test reports
- Risk analysis of the (other) processor
- Process descriptions
- Relevant policies and regulations
- Training materials for employees
- User manual
- Contracts with other processors (in particular: requirements for TOM), if applicable

Testing tools / application aids:

The relevant test modules of the German BSI can be used as a guideline for checks. These both reflect the state of the art and differentiate between measures according to

©EuroPriSe Cert GmbH

risk classes. In addition, ENISA offers relevant support and, together with TeleTrusT, provides a practical guide to the state of the art.

End of guidance

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.

Guidance

Relevant articles of the GDPR:

Art. 5 par. 1 lit. f) and Art. 32 par. 1 lit. b) GDPR

Introduction / Overview:

If passwords are used to authenticate users (or machines), specific security aspects must be taken into account. These include, in particular, those concerning the management, modification and revocation / invalidation of passwords. The choice of password complexity, mechanisms for changing passwords and measures for securely storing passwords must be made in accordance with the circumstances. This may also include the technical solution of multi-factor authentication.

End of guidance

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.

Guidance

Evaluation methods:

Typically, the following evaluation methods are used:

- On-site audit to monitor effectiveness

 ©EuroPriSe Cert GmbH

- Interviews with supervisors and employees
- Document review
- Consideration of relevant other certifications
- Test access / account

Documents:

Typically, the following documents are relevant in this respect:

- Relevant third-party certifications with associated test reports
- Risk analysis of the (other) processor
- Process descriptions
- Relevant policy and regulations
- Training materials for employees
- User manual
- Contracts with other processors (in particular: requirements for TOM), if applicable

Testing tools / application aids:

The relevant test modules of the German BSI can be used as a guideline for checks. These both reflect the state of the art and differentiate between measures according to risk classes. In addition, ENISA offers relevant support and, together with TeleTrusT, provides a practical guide to the state of the art.

End of guidance

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.

Guidance

Relevant articles of the GDPR:

Art. 5 par. 1 lit. f) and Art. 32 par. 1 lit. b) GDPR

Introduction / Overview:

Access control must be managed. This includes the definition and documentation of access rights and the technical implementation and configuration of access controls. In this respect, all types of access control (physical and logical) are affected, as well as cases where it is difficult to separate the management of access and access permissions from that of authentication methods (such as the use of mechanical keys, where access permissions can only be revoked by withdrawing the corresponding keys).

End of guidance

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.

Guidance

Evaluation methods:

Typically, the following evaluation methods are used:

- On-site audit to monitor effectiveness
- Interviews with supervisors and employees
- Document review
- Consideration of relevant other certifications
- Test access / account

Documents:

Typically, the following documents are relevant in this respect:

- Relevant third-party certifications with associated test reports
- Risk analysis of the (other) processor
- Process descriptions
- Relevant policies and regulations
- Training materials for employees
- User manual
- (Excerpt) inventory list
- Contracts with other processors (in particular: requirements for TOM), if applicable

Testing tools / application aids:

The relevant test modules of the German BSI can be used as a guideline for checks. These both reflect the state of the art and differentiate between measures according to risk classes. In addition, ENISA offers relevant support and, together with TeleTrusT, provides a practical guide to the state of the art.

End of guidance

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.

Guidance

Relevant articles of the GDPR:

Art. 5 par. 1 lit. a) + para. 2 and Art. 32 par. 1 GDPR

Introduction / Overview:

Logging access to and (further) processing of personal data is an important measure to ensure the verifiability (auditability) of processing. Log files and log data usually contain personal data relating to both the data subjects (persons whose data are processed for the intended or actual use of the processing operations) and the persons who process these data (e.g. employees of the processor). The latter may in certain cases also include the data subjects themselves (e.g. when they use a self-service that allows them, for example, to correct their own data).

End of guidance

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.

Guidance

Relevant articles of the GDPR:

(Art. 5 par. 1 lit. a) + par. 2 and Art. 32 par. 1 GDPR

Introduction / Overview:

Logging access to personal data and its (further) processing is an important measure to ensure the verifiability (auditability) of processing.

End of guidance

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,

©EuroPriSe Cert GmbH

- 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").

Guidance

Evaluation methods:

Typically, the following evaluation methods are used:

- On-site audit to monitor effectiveness
- Interviews with supervisors and employees
- Document review
- Consideration of relevant other certifications
- Test access / account
- Checking the log files

Documents:

Typically, the following documents are relevant in this respect:

- Relevant third-party certifications with associated test reports
- Risk analysis of the (other) processor
- Process descriptions
- Relevant policies and regulations
- Contracts with other processors (in particular: requirements for TOM), if applicable

Testing tools / application aids:

The relevant test modules of the German BSI can be used as a guideline for checks. These both reflect the state of the art and differentiate between measures according to risk classes. In addition, ENISA offers relevant support and, together with TeleTrusT, provides a practical guide to the state of the art.

End of guidance

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.

Guidance

Relevant articles of the GDPR:

Art. 5 par. 1 lit. a) + par. 2 and Art. 32 par. 1 GDPR

Introduction / Overview:

Due to the classification of log data as personal data, log data must be secured by technical and organisational measures.

End of guidance

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.

Guidance

Evaluation methods:

Typically, the following evaluation methods are used:

- On-site audit to monitor effectiveness
- Interviews with supervisors and employees
- Document review
- Consideration of relevant other certifications
- Test access / account

Documents:

Typically, the following documents are particularly relevant:

- Relevant third-party certifications with associated test reports
- Risk analysis of the (other) processor
- Process descriptions
- Relevant policies and regulations
- Training materials for employees
- Contracts with other processors (in particular: requirements for TOM), if applicable

Testing tools / application aids:

©EuroPriSe Cert GmbH

The relevant test modules of the German BSI can be used as a guideline for checks. These both reflect the state of the art and differentiate between measures according to risk classes. In addition, ENISA offers relevant support and, together with TeleTrusT, provides a practical guide to the state of the art.

End of guidance

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:”.

Guidance

Relevant articles of the GDPR:

Art. 5 par. 1 lit. f) and Art. 32 par. 1 lit. b) GDPR

Introduction / Overview:

Network and transport security concerns the security of the IT infrastructure and the security of the transmitted or transported data. While the first aspect usually concerns the entire infrastructure, the second aspect can be the subject of specific regulations that apply depending on the type of data being transmitted, the recipient, etc.

End of guidance

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.

Guidance

Evaluation methods:

CONFIDENTIAL

Typically, the following evaluation methods are used:

- On-site audit to monitor effectiveness
- Interviews with supervisors and employees
- Document review
- Consideration of relevant other certifications
- Test access / account

Documents:

Typically, the following documents are particularly relevant:

- Relevant third-party certifications with associated test reports
- Risk analysis of the (other) processor
- Process descriptions
- Relevant policies and regulations
- Training materials for employees
- Network topology
- Contracts with other processors (in particular: requirements for TOM), if applicable

Testing tools / application aids:

The relevant test modules of the German BSI can be used as a guideline for checks. These both reflect the state of the art and differentiate between measures according to risk classes. In addition, ENISA offers relevant support and, together with TeleTrusT, provides a practical guide to the state of the art.

Common testing tools such as

- https://www.ssllabs.com/ssltest/
- https://webbkoll.dataskydd.net/de
- https://owasp.org/www-project-top-ten/

End of guidance

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.

Guidance

Relevant articles of the GDPR:

Art. 5 par. 1 lit. f) and Art. 32 par. 1 lit. b) + c) GDPR

Introduction / Overview:

©EuroPriSe Cert GmbH

In addition to the integrity and confidentiality of personal data, their availability is resp. can also be an important protection goal. In this respect, it is not only about the availability of data, but also about the availability of the processing operations of the processor (including the associated hardware and software). A standard measure here is the creation of backup copies (backups), which must be supplemented by suitable storage measures and further organisational measures (e.g. recovery tests). Other measures that are particularly relevant with regard to business or other critical data (e.g. health data) are hardware redundancy measures (e.g. cold standby or hot standby), data mirroring (e.g. with the help of RAID systems or data replication) or the use of redundant data centres. Particularly in the case of ToEs that involve multiple processing operations, entire processes (including the associated data and hardware, but also personal know-how and knowledge, etc.) may need to be backed up in order to minimise breaches of availability due to incidents or data loss.

However, availability in the data protection context is never an "end in itself", but always has to be assessed with regard to the actual ToE. If personal data have completely "disappeared", this is certainly harmful from a processor's business point of view, but may not always be from the data subject's point of view, as can be seen in the example of "address collection for advertising purposes".

End of guidance

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.

Guidance

Relevant articles of the GDPR:

Art. 5 par. 1 lit. f) and Art. 32 par. 1 lit. b) GDPR

Introduction / Overview:

See above (chapter 2.1.4)

End of guidance

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[97]),

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

Guidance

Evaluation methods:

Typically, the following evaluation methods are used:

- On-site audit to monitor effectiveness
- Interviews with supervisors and employees
- Document review
- Consideration of relevant other certifications
- Test access / account

Documents:

Typically, the following documents are relevant in this respect:

- Relevant third-party certifications with associated test reports
- Risk analysis of the (other) processor
- Process descriptions
- Backup concept
- Relevant policies and regulations
- Training materials for employees
- Contracts with other processors (in particular: requirements for TOM), if applicable

Testing tools / application aids:

The relevant test modules of the German BSI can be used as a guideline for checks. These reflect both the state of the art and differentiate between measures according to risk classes.

End of guidance

2.1.4.2. Back-up mechanisms

Requirement in a nutshell:

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

Guidance

Relevant articles of the GDPR:

Art. 5 par. 1 lit. f) and Art. 32 par. 1 lit. b) + c) GDPR

Introduction / Overview:

See above (chapter 2.1.4)

End of guidance

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.

Guidance

Evaluation methods:

Typically, the following evaluation methods are used:

- On-site audit to monitor effectiveness
- Interviews with supervisors and employees
- Document review
- Consideration of relevant other certifications
- Test access / account

Documents:

Typically, the following documents are particularly relevant:

- Relevant third-party certifications with associated test reports
- Risk analysis of the (other) processor
- Process descriptions
- Backup concept
- Relevant policies and regulations
- Training materials for employees
- Contracts with other processors (in particular: requirements for TOM), if applicable

Testing tools / application aids:

The relevant test modules of the German BSI can be used as a guideline for checks. These both reflect the state of the art and differentiate between measures according to risk classes.

End of guidance

2.1.4.3. Backup storage

Requirement in a nutshell:

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

Guidance

Relevant articles of the GDPR:

Art. 5 par. 1 lit. f) and Art. 32 par. 1 lit. b) + c) GDPR

Introduction / Overview:

See above (chapter 2.1.4)

End of guidance

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).

Guidance

Evaluation methods:

Typically, the following evaluation methods are used:

- On-site audit to monitor effectiveness
- Interviews with supervisors and employees
- Document review
- Consideration of relevant other certifications
- Test access / account

Documents:

Typically, the following documents are particularly relevant:

- Relevant third-party certifications with associated test reports
- Risk analysis of the processor
- Process descriptions
- Backup concept
- Relevant policies and regulations
- Training materials for employees
- Contracts with other processors (in particular: requirements for TOM), if applicable

Testing tools / application aids:

The relevant test modules of the German BSI can be used as a guideline for checks. These both reflect the state of the art and differentiate between measures according to risk classes. In addition, ENISA offers relevant support and, together with TeleTrusT, provides a practical guide to the state of the art.

End of guidance

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:”.

Guidance

Relevant articles of the GDPR:

Art. 5 par. 1 lit. f) and Art. 32 par. 1 lit. b) + c) GDPR

Introduction / Overview:

See above (chapter 2.1.4)

End of guidance

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,
- 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.

Guidance

Evaluation methods:

Typically, the following evaluation methods are used:

- On-site audit to monitor effectiveness
- Interviews with supervisors and employees
- Document review
- Consideration of relevant other certifications
- Test access / account

Documents:

Typically, the following documents are particularly relevant:

- Relevant third-party certifications with associated test reports
- Risk analysis of the (other) processor
- Process descriptions
- Backup concept
- Relevant policies and regulations
- Training materials for employees
- Contracts with other processors (in particular: requirements for TOM), if applicable

Testing tools / application aids:

 ©EuroPriSe Cert GmbH

The relevant test modules of the German BSI can be used as a guideline for checks. These both reflect the state of the art and differentiate between measures according to risk classes. In addition, ENISA offers relevant support and, together with TeleTrusT, provides a practical guide to the state of the art.

End of guidance

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.

Guidance

Relevant articles of the GDPR:

Art. 5 par. 2, Art. 24 par. 1+2, Art. 32 par. 1 lit. d) and Art. 39 par. 1 lit. b) GDPR

Introduction / Overview:

To ensure the sustainability of the implemented data protection measures, these measures must be embedded in a management system. Important aspects of data protection and IT security measures are: Aspects of the relevant data protection and IT security policies, the selection and justification of measures, detailed documentation as well as a review of the measures implemented. Furthermore, specific measures may be relevant, such as the obligation of employees to maintain confidentiality.

In the context of a certification of processing operations by processors according to EuroPriSe, however, the entire data protection management system of a processor is not put to the test, but only aspects that are directly related to the ToE are considered. This may also extend to other processors, if applicable.

In detail, the specific requirements listed below must be met.

End of guidance

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.

Guidance

Relevant articles of the GDPR:

Art. 24 par. 1, Art. 32 par. 1 and Art. 35 GDPR

Introduction / Overview:

Technical and organisational data protection measures must be selected with regard to the risk of a breach of data protection rules (cf. Art. 32 par. 1 read in conjunction with recital 83, sentence 1 GDPR). This requires an assessment of the state of the art, the costs of implementation and the nature, scope, context and purposes of processing, as

©EuroPriSe Cert GmbH

well as the risk of varying likelihood and severity for the rights and freedoms of natural persons (cf. Art. 32 par. 1 GDPR).

If the processing of personal data resulting from the intended use of the processing operations to be certified is likely to result in a high risk to the rights and freedoms of natural persons by virtue of the nature, scope, context and purposes of the processing, the requirements regarding the conduct of a data protection impact assessment (DPIA) must be verified not only from a legal[98] but also from a technical point of view.

End of guidance

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.[99]

Guidance

Evaluation methods:

Typically, the following evaluation methods are used:

- On-site audit to monitor effectiveness
- Interviews with supervisors and employees
- Document review
- Consideration of relevant other certifications
- Test access / account

Documents:

Typically, the following documents are relevant in this respect:

- Relevant third-party certifications with associated test reports
- Risk analysis / DPIA of the (other) processor

[98] See also chapter 1.2.2 of this criteria catalogue (at details on the subject of the requirement, no. 6).

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

- Process descriptions
- Relevant policies and regulations
- Training materials for employees
- User manual
- Contracts with other processors (in particular: requirements for TOM), if applicable

Testing tools / application aids:

The relevant instructions of the German BSI, ENISA/TeleTrusT or the standard data protection model (SDM) for conducting risk analyses can be used as a guide during reviews. See also chapter 4 of the methodology compendium P.

End of guidance

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.

Guidance

Relevant articles of the GDPR:

Art. 5 par. 1 lit. a) + par. 2 and Art. 32 par. 1 GDPR

Introduction / Overview:

The basis for proper implementation of technical and organisational measures is documentation of the measures already implemented or yet to be implemented. Such documentation can be used to compare the planned measures with the currently implemented measures. The selection of measures must be based on the risk analysis (see chapter 2.1.5.1 as well as chapter 4 of the methodology compendium P). As this document is likely to contain information classified as confidential, it will usually not be publicly available. Therefore, the tasks and duties of users and administrators are to be presented in a separate document (see the following subchapter 2.1.5.3).

End of Guidance

Requirement in detail:

The processor SHALL demonstrate that:

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

Guidance

Evaluation methods:

Typically, the following evaluation methods are used:

- On-site audit to monitor effectiveness
- Interviews with supervisors and employees
- Document review
- Consideration of relevant other certifications

Documents:

Typically, the following documents are relevant in this respect:

- Relevant third-party certifications with associated test reports
- Risk analysis of the (other) processor
- Process descriptions
- Relevant policies and regulations
- Training materials for employees
- Current list of technical and organisational measures
- Contracts with other processors (in particular: requirements for TOM), if applicable

Testing tools / application aids:

The relevant instructions of the German BSI, ENISA/TeleTrusT or the standard data protection model (SDM) can be used as a guide during reviews.

End of guidance

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.

Guidance

Relevant articles of the GDPR:

Art. 5 par. 1 lit. a) + par. 2 and Art. 32 par. 1 GDPR

Introduction / Overview:

In order for users and administrators (here meaning the processor's own employees as well as employees of other processors) to know their tasks and obligations, these must be documented (e.g. in the form of work instructions or process descriptions - SOPs). The corresponding documentation must be easily accessible for users and administrators.

End of guidance

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).

Guidance

Evaluation methods:

Typically, the following evaluation methods are used:

- On-site audit to monitor effectiveness
- Interviews with supervisors and employees
- Document review
- Consideration of relevant other certifications

Documents:

Typically, the following documents are relevant in this respect:

- Relevant third-party certifications with associated test reports
- Risk analysis of the (other) processor
- Process descriptions
- Relevant policies and regulations
- Training materials for employees
- Work instructions
- Current list of technical and organisational measures

Testing tools / application aids:

The relevant instructions of the German BSI, ENISA/TeleTrusT or the standard data protection model (SDM) can be used as a guide during reviews.

End of guidance

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.

Guidance

Relevant articles of the GDPR:

Art. 5 par. 1 lit. a) + par. 2 and Art. 32 par. 1 GDPR

Introduction / Overview:

In order to be able to assess all data processing operations and evaluate their compliance with EU data protection law, an inventory of hardware, software, data and media used for personal data processing activities (if any) is required. Since some of this information is

also required for the record of processing activities (cf. chapter 1.1.1), the relevant information may be summarised in a single document.

End of guidance

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.

Guidance

Evaluation methods:

Typically, the following evaluation methods are used:

- On-site audit to monitor effectiveness
- Interviews with supervisors and employees
- Document review
- Consideration of relevant other certifications

Documents:

Typically, the following documents are relevant in this respect:

- Relevant third-party certifications with associated test reports
- Risk analysis of the (other) processor
- Process descriptions
- Relevant policies and regulations
- Training materials for employees

Testing tools / application aids:

The relevant instructions from the German BSI and ENISA/TeleTrusT can be used as a guide during checks.

End of guidance

2.1.5.5. Storage media management

Requirement in a nutshell:

The processor SHALL ensure the controlled handling of storage media.

Guidance

Relevant articles of the GDPR:

 ©EuroPriSe Cert GmbH

Art. 5 par. 1 lit. a) + par. 2 and Art. 32 par. 1 GDPR

Introduction / Overview:

Media on which personal data can be stored include CDs, DVDs, tapes and USB data carriers.

End of guidance

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.

Guidance

Evaluation methods:

Typically, the following evaluation methods are used:

- On-site audit to monitor effectiveness
- Interviews with supervisors and employees
- Document review
- Consideration of relevant other certifications

Documents:

In particular, the following documents are relevant:

- Relevant third-party certifications with associated test reports
- Risk analysis of the (other) processor
- Process descriptions
- Relevant policies and regulations

CONFIDENTIAL

- Training materials for employees
- Media register

Testing tools / application aids:

The relevant instructions from the German BSI and ENISA/TeleTrusT can be used as a guide during checks.

End of guidance

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.

Guidance

Relevant articles of the GDPR:

Art. 28 par. 3 lit. b), Art. 29 and Art. 39 par. 1 lit. a) + b) GDPR

Introduction / Overview:

Persons who have access to personal data are usually employees of the processor or employees of other processors. They must have committed themselves to confidentiality or be subject to a statutory obligation of confidentiality. Such confidentiality obligations must also apply beyond the termination of the respective employment relationship. On the subject of confidentiality, see also chapter 1.2.2.

End of guidance

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).

Guidance

Evaluation methods:

Typically, the following evaluation methods are used:

- On-site audit to monitor effectiveness
- Interviews with supervisors and employees

CONFIDENTIAL

- Document review
- Consideration of relevant other certifications

Documents:

Typically, the following documents are particularly relevant:

- Relevant third-party certifications with associated test reports
- Risk analysis of the (other) processor
- Relevant policies and regulations
- Training materials for employees
- Contracts with other processors (in particular: requirements for TOM), if applicable

Testing tools / application aids:

The relevant instructions from the German BSI and ENISA/TeleTrusT can be used as a guide during checks.

End of guidance

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.

Guidance

Relevant articles of the GDPR:

Art. 28 par. 3 lit. h), Art. 32 par. 1 lit. d) and Art. 35 GDPR

Introduction / Overview:

In order to assess their (ongoing) effectiveness, technical and organisational data protection measures must be regularly reviewed and evaluated. Such audits can be carried out either by employees of the organisation or by external auditors.

End of guidance

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.

Guidance

Evaluation methods:

Typically, the following evaluation methods are used:

- On-site audit to monitor effectiveness

- Interviews with supervisors and employees
- Document review
- Consideration of relevant other certifications

Documents:

Typically, the following documents are particularly relevant:

- Relevant third-party certifications with associated test reports
- Annual audit programme
- IS and/or DP audit reports
- Minutes of management reviews

Testing tools / application aids:

N/A

End of guidance

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.

Guidance

Relevant articles of the GDPR:

Art. 32 par. 1 lit. d) and Art. 33 f. GDPR

Introduction / Overview:

An organisation must have management processes in place to respond to security or privacy incidents and identified vulnerabilities. This includes documentation of such incidents, the remediation resp. recovery actions and notification of customers / data subjects thereof (in this respect, reference is made to Art. 33 par. 2 GDPR according to which the processor must notify the controller without undue delay after becoming aware of a personal data breach). The objective of such incident management is to enable a learning process aimed at preventing further incidents and to support those responsible in preventing such incidents. In addition, procedures must be in place to address security vulnerabilities before they result in concrete security incidents. This chapter overlaps with chapter 1.2.2.

End of guidance

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).

Guidance

Evaluation methods:

Typically, the following evaluation methods are used:

- On-site audit to monitor effectiveness
- Interviews with supervisors and employees
- Document review
- Consideration of relevant other certifications

Documents:

Typically, the following documents are particularly relevant:

- Relevant third-party certifications with associated test reports
- Minutes of the management reviews
- Incident list
- Contracts with other processors (in particular: requirements for TOM), if applicable

Testing tools / application aids:

- Art. 29 WP (endorsed by the EDPB): Guidelines on Personal data breach notification under Regulation 2016/679 (wp250rev.01) (cf. in particular chapter II.A.4.: "Processor obligations").
- EDPB: Guidelines 01/2021 on Examples regarding Data Breach Notification

End of guidance

2.1.5.9. Test and release

Requirement in a nutshell:

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

Guidance

Relevant articles of the GDPR:

Art. 32 par. 1 lit. d) GDPR

Introduction / Overview:

Before IT processing operations are used, they must be tested and formally released. Only test data or anonymous data may be used for such tests. Real data, on the other hand, may only be used in exceptional cases. Tests that have been carried out must be documented. The tests were not only to relate to the intended use of the respective IT component, but also to attempts at unauthorised and/or improper use (e.g. use of incorrect input data). Testing and release can be combined with a data protection impact assessment (cf. chapter 3 of the methodology compendium P; see also chapter 2.1.8 of this criteria catalogue - documentation of the service from the customer's perspective).

End of guidance

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.

Guidance

Evaluation methods:

Typically, the following evaluation methods are used:

- On-site audit to monitor effectiveness
- Interviews with supervisors and employees
- Document review
- Consideration of relevant other certifications

Documents:

Typically, the following documents are particularly relevant:

- Relevant third-party certifications with associated test reports
- Process descriptions
- Relevant policies and regulations
- Training materials for employees

Testing tools / application aids:

The relevant test modules of the German BSI can be used as a guideline for checks. These reflect both the state of the art and differentiate between measures according to risk classes.

End of guidance

©EuroPriSe Cert GmbH

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.

Guidance

Relevant articles of the GDPR:

Art. 5 par. 1 lit. e), Art. 17 and Art. 19 GDPR

Introduction / Overview:

Upon completion of the processing services, the processor must delete and/or return all personal data and any copies made. The processor must also assist the controller in fulfilling its obligation to respond to data subjects' requests for erasure. Furthermore, the issue of erasure is also relevant when personal data are no longer needed for the purposes for which they are processed. Finally, the processor must also ensure the proper disposal of hardware, software or media on which personal data are stored.

End of guidance

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.

CONFIDEN

- 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.

Guidance

Evaluation methods:

Typically, the following evaluation methods are used:

- On-site audit to monitor effectiveness
- Interviews with supervisors and employees
- Document review
- Consideration of relevant other certifications

Documents:

Typically, the following documents are particularly relevant:

- Relevant third-party certifications with associated test reports
- Process descriptions
- Relevant policies and regulations
- Training materials for employees
- Contracts with other processors (in particular: requirements for TOM), if applicable

Testing tools / application aids:

The relevant instructions from the German BSI, ENISA/TeleTrusT and the standard data protection model (SDM) can be used as a guide during reviews.

End of guidance

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.

Guidance

Relevant articles of the GDPR:

Art. 5 par. 1 lit. d) + f), Art. 17 and Art. 32 par. 1 lit. b) GDPR

Introduction / Overview:

When temporary files or data are created, access to them must be controlled in the same way as access to other types of personal data. Temporary data must be deleted when it is no longer needed for the purposes for which it was created.

End of guidance

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.

Guidance

Evaluation methods:

Typically, the following evaluation methods are used:

- On-site audit to monitor effectiveness
- Interviews with supervisors and employees
- Document review
- Consideration of relevant other certifications
- Test access / account

Documents:

Typically, the following documents are particularly relevant:

- Relevant third-party certifications with associated test reports
- Process descriptions
- Relevant policies and regulations
- Training materials for employees
- Work instructions
- Contracts with other processors (in particular: requirements for TOM), if applicable

Testing tools / application aids:

The relevant instructions from the German BSI and ENISA/TeleTrusT can be used as a guide during reviews.

End of guidance

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.

Guidance

Relevant articles of the GDPR:

Art. 5 par. 1 lit. a) + par. 2 and Art. 32 par. 1 GDPR

Introduction / Overview:

Customers of processing operations by processors to be certified according to EuroPriSe usually qualify as controllers and must therefore comply with EU data protection law. To do so, they need information that enables them to fulfil their legal obligations.

End of guidance

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.

Guidance

Evaluation methods:

Typically, the following evaluation methods are used:

- On-site audit to monitor effectiveness
- Interviews with supervisors and employees
- Document review
- Consideration of relevant other certifications
- Test access / account

Documents:

Typically, the following documents are particularly relevant:

- Customer documentation, here performance description of the processing operations
- Data protection leaflet
- Data processing agreement (DPA)
- TOM documents

Testing tools / application aids:

CONFIDENTIAL

The relevant instructions from the German BSI and ENISA/TeleTrusT can be used as a guide during reviews.

End of guidance

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.

Guidance

Relevant articles of the GDPR:

Art. 5 par. 1 lit. f) and Art. 32 par. 1 lit. a) GDPR

Introduction / Overview:

The GDPR explicitly identifies encryption as an (important technical) measure to ensure a level of security appropriate to the risks represented by the processing. Encryption may be necessary, for example, when personal data is transferred over a network or stored on a mobile device such as a notebook. Encryption may also be used to implement access control mechanisms (e.g. for databases and backup storage).

End of guidance

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).

Guidance

Evaluation methods:

Typically, the following evaluation methods are used:

CONFIDENTIAL

- On-site audit to monitor effectiveness
- Interviews with supervisors and employees
- Document review
- Consideration of relevant other certifications
- Test access / account

Documents:

Typically, the following documents are particularly relevant:

- Relevant third-party certifications with associated test reports
- Process descriptions
- Relevant policies and regulations
- Training materials for employees
- Work instructions
- Contracts with other processors (in particular: requirements for TOM), if applicable

Testing tools / application aids:

The relevant instructions from the German BSI and ENISA/TeleTrusT can be used as a guide during reviews.

End of guidance

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 **Fehler! Verweisquelle konnte nicht gefunden werden.**. of this criteria catalogue). 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.

Guidance

Relevant articles of the GDPR:

Art. 4 No. 5, Art. 25 par. 1 and Art. 32 par. 1 lit. a) GDPR

Introduction / Overview:

For anonymisation[100] and/or pseudonymisation[101] of personal data, effective methods must be used, in particular to prevent detection of pseudonyms / any other re-identification

[100] Attribution of data to a specific person after anonymisation is no longer possible, at least not without disproportionate effort.

[101] Attribution of data to a specific person after pseudonymisation is only possible with the use of additional information (cf. Art. 4 No. 5 GDPR).

resp. to ensure that such re-identification requires a disproportionate effort. Information that can be used to detect pseudonyms (especially so-called attribution rules) must be protected.

End of guidance

Requirement in detail:

N/A

Guidance

Evaluation methods:

Typically, the following evaluation methods are used:

- On-site audit to monitor effectiveness
- Interviews with supervisors and employees
- Document review
- Consideration of relevant other certifications
- Test access / account

Documents:

Typically, the following documents deal with the issue:

- Relevant third-party certifications with associated test reports (if available)
- Process descriptions
- Relevant policies and regulations
- Training materials for employees
- Work instructions
- Contracts with other processors (in particular: requirements for TOM), if applicable

Testing tools / application aids:

The relevant instructions from the German BSI and ENISA/TeleTrusT can be used as a guide during reviews.

End of guidance

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 catalogue. 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[102] 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.

Guidance

Relevant articles of the GDPR:

Art. 28 par. 3 sentence 2 lit. e) GDPR read in conjunction with Art. 12-14 GDPR

Background:

Article 28 par. 3 sentence 2 lit. e) GDPR obliges the processor to support the controller with technical and organisational measures with regard to the rights of the data subjects.

End of guidance

Requirement in detail:

[102] Cf. chapter 1.2.1 of this criteria catalogue.

©EuroPriSe Cert GmbH

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 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

Guidance

Relevant documents:

1. Relevant work instructions and process descriptions
2. List of other processors
3. TOM document

Relevant evaluation methods:

Document review, interviews

Application/interpretation aids:

- Art. 29 WP (endorsed by the EDPB): Guidelines on transparency under Regulation 2016/679 (WP 260 rev.01 - cf. in particular par. 23 ff.: "Information to be provided to the data subject - Articles 13 & 14")
- DE: Kurzpapier No. 10 der DSK

End of guidance

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

©EuroPriSe Cert GmbH

- 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.

Guidance

Relevant articles of the GDPR:

Art. 28 par. 3 sentence 2 lit. e) GDPR read in conjunction with Art. 15 GDPR

Background:

Article 28 par. 3 sentence 2 lit. e) GDPR obliges the processor to support the controller with technical and organisational measures with regard to the rights of the data subjects.

End of guidance

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

Guidance

Relevant documents:

Relevant work instructions and process descriptions

Relevant evaluation methods:

Document review, interviews

Application/interpretation aids:

- EDPB: Guidelines 01/2022 on data subject rights - Right of access
- DE: Kurzpapier No. 6 der DSK

End of guidance

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

©EuroPriSe Cert GmbH

- 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.

Guidance

Relevant articles of the GDPR:

Art. 28 par. 3 sentence 2 lit. e) GDPR read in conjunction with. Art. 16 GDPR

Background:

Article 28 par. 3 sentence 2 lit. e) GDPR obliges the processor to support the controller with technical and organisational measures with regard to the rights of the data subjects.

End of guidance

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

Guidance

Relevant documents:

Relevant work instructions and process descriptions

Relevant evaluation methods:

Document review, interviews

Application/interpretation aids:

N/A

End of guidance

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

©EuroPriSe Cert GmbH

- 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.

Guidance

Relevant articles of the GDPR:

Art. 28 par. 3 sentence 2 lit. e) GDPR read in conjunction with Art. 17 GDPR

Background:

Article 28 par. 3 sentence 2 lit. e) GDPR obliges the processor to support the controller with technical and organisational measures with regard to the rights of the data subjects.

End of guidance

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

Guidance

Relevant documents:

Relevant work instructions and process descriptions

Relevant evaluation methods:

Document review, interviews

Application/interpretation aids:

- EDPB: Guidelines 5/2019 on the criteria of the Right to be Forgotten in the search engines cases under the GDPR
- DE: Kurzpapier No. 11 of der DSK

End of guidance

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,

©EuroPriSe Cert GmbH

- 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.

Guidance

Relevant articles of the GDPR:

Art. 28 par. 3 sentence 2 lit. e) GDPR read in conjunction with Art. 18 GDPR

Background:

Article 28 par. 3 sentence 2 lit. e) GDPR obliges the processor to support the controller with technical and organisational measures with regard to the rights of the data subjects.

End of guidance

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

Guidance

Relevant documents:

Relevant work instructions and process descriptions

Relevant evaluation methods:

Document review, interviews

Application/interpretation aids:

N/A

End of guidance

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,

©EuroPriSe Cert GmbH

- 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.

Guidance

Relevant articles of the GDPR:

Art. 28 par. 3 sentence 2 lit. e) GDPR read in conjunction with Art. 20 GDPR

Background:

Article 28 par. 3 sentence 2 lit. e) GDPR obliges the processor to support the controller with technical and organisational measures with regard to the rights of the data subjects.

End of guidance

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

Guidance

Relevant documents:

Relevant work instructions and process descriptions

Relevant evaluation methods:

Document review, interviews

Application/interpretation aids:

Art. 29 WP (endorsed by the EDPB): Guidelines on the right to “data portability” (WP 242 rev.01)

End of guidance

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.

Guidance

Relevant articles of the GDPR:

Art. 28 par. 3 sentence 2 lit. e) GDPR read in conjunction with Art. 21 GDPR

Background:

Article 28 par. 3 sentence 2 lit. e) GDPR obliges the processor to support the controller with technical and organisational measures with regard to the rights of the data subjects.

End of guidance

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

Guidance

Relevant documents:

Relevant work instructions and process descriptions

Relevant evaluation methods:

Document review, interviews

Application/interpretation aids:

N/A

End of guidance

©EuroPriSe Cert GmbH