Athens, 06-08-2020

Prot. no.: G/EX/5511/06-08-2020

PRINCIPLE OF DATA PROTECTION

OF A PERSONAL CHARACTER

A P O F A S H 25/2020

The Personal Data Protection Authority (the Authority) met, following an invitation

of its President, in a regular meeting at its headquarters on Wednesday 05.08.2020, in

continuation of the meeting from 22.07.2020, in order to examine the issue which

concerns the maintenance or modification of the plan of supplementary requirements

for the accreditation of bodies that grant certifications to managers

processors and processors in accordance with articles 42 and 43 thereof

Regulation (EU) 2016/679 for the protection of natural persons against

processing of personal data

(General Regulation

of Data Protection - GDPR) following the relevant opinion numbered 22/2020

issued by the European Data Protection Board (Board).

The President of the Authority, Konstantinos Menudakos, and the regular members were present

Spyridon Vlachopoulos, Konstantinos Lambrinoudakis, as rapporteur and

Charalambos Anthopoulos, also as rapporteur. The meeting was also attended by

by order of the President, without the right to vote, the expert scientists Euphrosyne

Siougle and Konstantinos Limniotis, IT auditors, as assistant rapporteurs

as well as Georgia Palaiologou, an employee of the Administrative Department

Affairs, as secretary.

The Authority took into account the following:

With its decision number 8/2020, the Authority decided to draw up a plan in

which are defined as complementary, in relation to the EN-ISO/IEC standard

17065/2012, requirements for the accreditation of certification bodies according to

1

provided for in articles 43 par. 1 item b', 43 par. 3 and 57 par. 1 item his web

GDPR as well as in article 37 par. 1 of law 4624/2019. The Authority, before its approval

in that plan, apply the coherence mechanism referred to in the article

63 and announced this plan to the Council, in accordance with article 64 par. 1

point c of the GDPR. The Council, following a written procedure (written

procedure), which is provided for in article 24 par. 3 of the internal Regulation

and which was completed on July 23, 2020, issued opinion 22/2020 regarding

with the said plan of the Authority based on article 64 par. 3 of the GDPR. With the opinion

this, which was sent to the Authority electronically on July 29, 2020,

The Council asked the Authority to modify the plan in question based on

including recommendations for its coherent implementation

accreditation of certification bodies.

The Authority, after hearing the rapporteurs and assistant rapporteurs, who at

then they left, and after a thorough discussion

CONSIDERED ACCORDING TO THE LAW

1. According to article 9 of Law 4624/2019, which aims – among other things

- the adoption of GDPR implementation measures, the supervision of the implementation of the provisions

of the GDPR in the Greek Territory is exercised by the Authority.

2. According to article 15 paragraph 10 of Law 4624/2019 "The regulatory acts of

Authority, for which there is no provision for their publication in its Gazette

Government, are published on the website of the Authority".

3. According to article 43 paragraph 6 of the GDPR "The requirements of paragraph 3

of this article (…) are made public by the supervisory authority in a fluent manner

accessible format. The supervisory authorities shall also transmit these requirements

and the criteria in the Data Protection Board".

4. According to article 57 par. 1 item website of the GDPR, the Authority "(...) plans and

publishes the accreditation requirements (…) certification body according to

article 43 (…)"

5. According to article 64 par. 1, 3, 6, 7 and 8 of the GDPR:

"(par. 1) The Council issues an opinion whenever a competent supervisory authority intends

to adopt any of the following measures. For this purpose, the competent

supervisory authority announces the draft decision to the Council, when: (…) c)

aims to approve the requirements for the accreditation (…) body

certification in accordance with article 43 paragraph (…)".

"(par. 3) In the cases referred to in paragraphs 1 and 2, the Council

Data Protection issues an opinion on the subject matter

is submitted, since it has not already issued an opinion on the same subject. The opinion

it is issued within a period of eight weeks by a simple majority of the members

of the Data Protection Board. This deadline can be extended

by a further six weeks, taking into account the complexity of the matter

(...)".

"(par. 6) The competent supervisory authority referred to in paragraph 1 does not approve

the draft decision referred to in paragraph 1 within the period which

referred to in paragraph 3'.

"(par. 7) The competent supervisory authority referred to in paragraph 1 receives

taking into account the opinion of the Data Protection Board and, within two

weeks from the receipt of the opinion, it notifies its President

Data Protection Board by electronic means as to whether it will keep

or will amend the draft decision and, where applicable, the

amended draft decision, using a standard format'.

"(par. 8) When the competent supervisory authority referred to in paragraph 1

informs the President of the Data Protection Board, within it

deadline referred to in paragraph 7 of this article, that no

intends to follow the opinion of the Data Protection Board, at

in whole or in part, providing the relevant justification, Article 65 is applied

paragraph 1'.

6. In view of the above, the Authority, after taking into account and examining the recommendations,

including incentives, Council opinion 22/2020,

unanimously held that all the recommendations and encouragements of said opinion

must be accepted, the necessary changes must be made to their plan

of supplementary accreditation requirements, which he had originally submitted to

Council and to announce the amended plan to the Council, within it

deadline referred to in article 64 par. 7 of the GDPR.

3

7. For this purpose they were carried out on the draft of the supplementary ones

of accreditation requirements, which was drawn up with No. 8/2020

Decision of the Authority, the necessary changes to fulfill all of the

recommendations and encouragements of the Council's opinion 22/2020.

FOR THOSE REASONS

The Authority unanimously decides on the amendment of the supplementary plan

requirements for the accreditation of certification bodies, based on the recommendations and

of the encouragements of the Council's opinion 22/2020, and its announcement

of an amended plan to the Council, in accordance with article 64 par. 7 of the GDPR.

The amended plan will be published on the website of the Authority according to

with articles 43 par. 6 and 57 par. 1 item website of the GDPR as well as article 15 par.

10 of Law 4624/2019, after the completion of said procedure.

Following these, the amended supplementary accreditation requirements

is listed in the Annex to this decision.

The president

The Secretary

Konstantinos Menudakos

Paleologo Georgia

Annex

Additional requirements of the Personnel Data Protection Authority

Character for the accreditation of certification bodies according to the article

43 paragraph 1 letter b) and article 43 paragraph 3 GDPR in

combination with the EN-ISO/IEC 17065 standard

Contents

Introduction

The establishment of data protection certification mechanisms and seals and

data protection signals is provided for in Article 42 of the GDPR. The enactment

of these mechanisms can improve transparency and compliance with the

GDPR and allow data subjects to assess the level

data protection of the relevant products and services (reasonable

paragraph 100 of the GDPR).

The certification is granted by a certification body accredited for this purpose,

based on article 43 of the GDPR, to a controller or executor

processing, which has submitted its relevant processing to the mechanism

certification. The accreditation of certification bodies is of particular importance as

provides official confirmation of the relevant competence of these bodies

making it possible to develop trust in the certification mechanism.

According to article 37 paragraph 1 of Law 4624/2019, the accreditation of

bodies that grant certifications, in accordance with article 42 of the GDPR,

carried out by the National Accreditation System (hereafter E.SY.D.)

(www.esyd.gr), based on the EN-ISO/IEC 17065/2012 standard (henceforth ISO 17065) and

in accordance with the additional accreditation requirements set forth by

Personal Data Protection Authority (hereinafter the Data Protection Authority). The

E.SY.D. apply these additional requirements during the process

accreditation in conjunction with the ISO 17065 standard.

This document includes the supplementary accreditation requirements

set by the APDPH in relation to the ISO 17065 standard and in accordance with articles 43

paragraph 1 letter b) and 43 paragraph 3 of the GDPR.

These requirements are based on the proposed requirements of

of guidelines 4/20181 of the ESPD and must be applied to

combined with the ISO 17065 standard. The numbering of the units used

here corresponds to the numbering used in ISO 17065 and

ESPD guidelines. However, some of the sections of ISO 17065

are not included in this document. This means that for the specific

modules no additional accreditation requirements are set but applied

the requirements of the respective section of ISO 17065.

0. Prefix

At this point, the terms of cooperation between the APDPH and the E.SY.D.

in the context of the accreditation of certification bodies. More detailed terms

cooperation, roles, responsibilities and procedures in relation to accreditation will

be agreed between the APDPH and the E.SY.D.

The E.SY.D. must inform the APDPH in writing:

1) Regarding all accreditation requests submitted by the agencies

certification. In particular, the E.SY.D. provides the APDPH with a summary

description of the request, the name and contact details of the body

certification, the certification scheme for which accreditation is requested as well

1 'Guidelines 4/2018 regarding the accreditation of certification bodies based on article 43 of the General

Data Protection Regulation (2016/679)'

https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_4_2018_accreditation_en.pdf

and whether the certification criteria are approved by the competent supervisory authority

or the ESPD. In case the accreditation request is submitted to the E.SY.D. before

from the final approval of the certification criteria, the E.SY.D does not grant the

accreditation until the certification criteria receive final approval.

2) Regarding the reasons for granting or withdrawing the accreditation, before each

grant or withdrawal of accreditation. The information to the APDPH

includes at a minimum information about the brand and the

details of the certification body, the period of time of its granting

of accreditation, date of initial accreditation, start dates

and expiry of the current accreditation as well as the certification scheme which

accreditation is concerned.

3) For the actions taken regarding the revocation of the accreditation

in the event that the E.SY.D. be informed by the APDPH that they are not met

now the accreditation requirements or the certification body is in breach of the GDPR

and the provisions of Law 4624/2019 (Article 37 Par. 2 of Law 4624/2019).

The APDPH, if it decides, informs the E.SY.D within a reasonable period of time.

for any significant reasons for the certification body's non-compliance with

GDPR. In this case, the E.SY.D. may continue the process

accreditation, but does not complete it before its final relevant judgment

APDPH. The E.SY.D. is free to decide on its grant

accreditation. It should, however, take into account its final decision

APDPH without prejudice to the authority of APDPH to subsequently revoke the

accreditation, if deemed appropriate.

The information provided by APDPH to E.SY.D. in the framework of

accreditation process must be kept confidential.

The E.SY.D. must ensure full transparency to the APDPH regarding

the accreditation process in accordance with articles 43 par. 4 and 7, 58 par. 1 item

b) of the GDPR and article 37 par. 2 of law 4624/2019.

The staff of E.SY.D. who is responsible for the evaluations and involved

in the process of accreditation of certification bodies, must have

proven knowledge of GDPR and personal data protection.

1. Scope

This document contains the supplements to the ISO 17065 standard

accreditation requirements of the APDPH in accordance with articles 43 paragraph 1

point b) and 43 paragraph 3 of the GDPR, taking into account the guidelines

lines 4/2018 of the ESPD.

The scope of the ISO 17065 standard should be applied according to

the GDPR. The guidelines 4/2018 of the ESDP on accreditation

and the 1/2018 guidelines on certification provide

further information. The wider scope of the ISO 17065 standard which

covers products, processes and services shall not mitigate nor to

exceeds GDPR requirements. E.g. a governance mechanism cannot

to be the only element of a certification mechanism, given that the

certification must include the processing of personnel data

character, i.e. processing operations.

The scope of an authentication mechanism (for example, authentication

of cloud computing services processing operations), must be obtained

taken into account in the evaluation by the E.SY.D. during the process

accreditation,

especially in terms of criteria, expertise and

evaluation methodology.

Pursuant to Article 42(1) of the GDPR, the GDPR certification

applies only to processing operations by controllers and

the processors.

2. Regulatory reference documents

The GDPR takes precedence over ISO 17065. If the supplementary requirements

or through the certification mechanism reference is made to other ISO standards, these

are interpreted in accordance with the requirements set out in the GDPR.

3. Terms and Definitions

Accreditation guidelines terms and definitions apply

(ESPD 4/2018) and certification (ESPD 1/2018), which take precedence over

definitions of ISO standards.

For your convenience, the following basic definitions are listed: - "GDPR": Regulation 2016/679/EC - General Data Protection Regulation. - "ISO 17065": EN-ISO/IEC 17065/2012. - "Certification": the evaluation and certification by an impartial third party that the fulfillment of the certification criteria has been demonstrated in the context of the certification in accordance with Articles 42 and 43 of the GDPR for processing operations of controllers and processors. - "Accreditation": the third-party attestation regarding the activities of a conformity assessment body, which provides official assurance of the body's ability to carry out certifications pursuant to Articles 42 and 43 of the GDPR. This is the result of the assessment process of a certification body that is successfully certified (as part of the accreditation process). - "Certification body": a third-party conformity assessment body that administers certification schemes. - "Certification criteria": the criteria based on which the certification is carried out for a specific certification scheme. - "Certification scheme": certification system that concerns specific products, processes and services, for which the same requirements, 9 rules and procedures apply. It mainly includes the certification criteria and the evaluation methodology. - "Certification Mechanism": the system based on which a controller or processor is certified. This is an approved certification scheme which is available to the applicant along with a set of existing procedures. It is a service provided by an accredited certification body based on approved criteria and evaluation methodology. - "Object of assessment": the object of the certification. In the case of GDPR certification, these are the relevant processing operations for the evaluation and certification of which the data controller or processor submits an application. - "Applicant": the controller or processor, who submits an application for certification of his processing operations. - "Client": the controller or

processor, who has been certified. 4. General requirements for accreditation 4.1 Legal and contractual issues 4.1.1 Legal responsibility The certification body must be able to prove (at any time) to the E.SY.D. that it has up-to-date procedures that demonstrate compliance with the statutory responsibilities set out in the terms of accreditation, including additional requirements in relation to the implementation of the GDPR. As the certification body is itself a data controller/processor, it must be able to present evidence that its processes comply with the GDPR and Law 4624/2019 and that it implements measures specifically aimed at control and the management of the personal data of the client organization in the context of the certification process. The certification body must: - be able to provide evidence of GDPR compliance at any time during the accreditation process; - inform the E.SY.D. regarding violations of the GDPR or Law 4624/2019 found by the APDPH and/or the judicial authorities which may affect the accreditation; 10 - to ensure full transparency to the APDPH regarding the accreditation and certification procedures in accordance with articles 42 paragraph 7, 43 paragraph 4 of the GDPR, 58 paragraph 1 item b) and c) of the GDPR and article 37 paragraph 2 of Law 4624/2019. 4.1.2 Certification agreement In addition to paragraph 4.1.2.1 of the ISO 17065 standard, the legally enforceable agreement must be drawn up in writing. The certification body demonstrates that, in addition to the relevant requirements of the ISO 17065 standard, the certification agreements it concludes: 1. require the applicant to always comply with the general certification requirements within the meaning of paragraph 4.1.2.2 point a) of the ISO standard 17065 and with the certification criteria approved by the DPA or the EDPS in accordance with Articles 43 paragraph 2 point b) and 42 paragraph 5 of the GDPR; it concerns procedure 2. require the applicant to ensure full transparency for the DPA including confidential contract matters related to data protection compliance, in accordance with Articles 42 paragraph 7 and 58 paragraph 1 letter c) of the GDPR; certification, 3. do not reduce the applicant's responsibility for compliance with the GDPR and do not affect the duties and powers of the DPA in accordance with Article 42 paragraph 5 of the GDPR; 4. require the applicant to provide the body with a certificate of any information and access to the processing activities required to carry out the certification process in accordance with Article 42 paragraph 6 of the GDPR; 5. require the applicant to comply with applicable deadlines and procedures. The certification agreement must state that the deadlines and procedures resulting from, for example, the certification program or from other regulations must be respected and applied; 6. with regard to paragraph 4.1.2.2 item c) no. 1 of the ISO 17065 standard, set out the rules for validity, renewal and revocation in accordance with Articles 42(7) and 43(4) of the GDPR, including rules setting out appropriate time intervals for reassessment or review (periodicity) in accordance with Article 42(7) of GDPR and section

7.9 of the said requirements; 7. allow the certification body to disclose to the APDPH all the information necessary for the granting or revocation of the 11 certification and the reasons for the relevant decision, in accordance with articles 42 paragraph 8 and 43 paragraph 5 of the GDPR; 8. include rules regarding the necessary precautions, which must be applied for the investigation of complaints, in the sense of paragraph 4.1.2.2 item c) no. 2, and point j) of ISO 17065, in a transparent and easily accessible manner, while also including explicit statements about structures and procedures for handling complaints in accordance with Article 43 paragraph 2 point d) GDPR; 9. in addition to minimum requirements mentioned in paragraph 4.1.2.2 of the ISO 17065 standard, the certification agreement must include an explanation of the consequences of withdrawal or suspension of accreditation for the certification body as well as their impact on the client. In this case, the consequences for the customer must also be addressed by incorporating appropriate procedures into the management system of the certification body; 10. require the applicant to inform the certification body in case of significant changes in its actual or legal status and products , its procedures and services, which the certification concerns; 11. require the applicant to inform the certification body about any violations of the GDPR, which are found by the DPA and/or the judicial authorities and may affect the certification ˙ 12. define the terms and conditions that determine the duration of the certification process as well as the binding evaluation methods regarding the evaluation object. 4.1.3 Use of data protection seals and marks Certificates, seals and marks are only used in accordance with Articles 42 and 43 of the GDPR and the Accreditation and Certification Guidelines. 4.2 Management of impartiality The E.SY.D. ensures that, in addition to the requirements of paragraph 4.2 of the ISO 17065 standard: 1. the certification body complies with the additional requirements of the GDPR [according to article 43 paragraph 1 point b) of the GDPR] a. pursuant to Article 43(2)(a) of the GDPR, provides separate evidence of its independence. This applies in particular to the evidence relating to the funding of the certification body, insofar as it concerns the assurance of impartiality; 12 b. the certification body must provide separate evidence that its duties and obligations do not lead to a conflict of interest in accordance with Article 43(2)(e) of the GDPR; 2. the certification body has no relation or connection with the customer evaluating. The certifying body should not belong to the same group of companies nor be controlled in any way by the evaluating client. The certification body must ensure that there are no conflicts of interest and that it is able to demonstrate on a regular basis that it carries out its conformity assessment activities impartially, does not allow the exercise of commercial, financial and other pressures that jeopardize impartiality, as well as that it manages any conflicts of interest that may be identified. 4.3. Responsibility and funding The E.SY.D., apart from the requirements of paragraph 4.3.1 of the ISO 17065

standard, ensures on a regular basis that the certification body: 1. has assessed the risks related to the certification activities it carries out and has appropriate measures (e.g. insurance or reserves) to cover its obligations arising from its operations and areas of its activities in the geographical areas in which it operates, and 2. can sufficiently demonstrate that it has financial stability and the required resources for its operations. 4.6 Publicly available information The E.S.Y.D., in addition to the requirement of paragraph 4.6 of the ISO 17065 standard, requires from the certification body at least 1. all editions (current and previous) of the approved criteria used in the sense of article 42 paragraph 5 of the GDPR, as well as all certification procedures, to be published and easily accessible by the public, with a general reference to the corresponding period of validity; 2. information on complaint management procedures and appeals to be made public in accordance with article 43 paragraph 2 point d) of the GDPR. 13 5. Structural requirements, article 43 paragraph 4 of the GDPR ["correct" assessment] 5.1 Organizational structure and senior management The E.S.D., in addition to the requirements of paragraph 5.1.3 of the ISO 17065 standard, must require by the certification body to appoint a person with overall control and responsibility to oversee data protection in relation to the assessment, decisions and supervision of the certification. 6. Required resources 6.1 Personnel of the certification body ESYD, in addition to the requirement of paragraph 6 of the ISO 17065 standard, ensures that the personnel of each certification body: 1. have demonstrated that they have appropriate and lasting expertise (knowledge and experience) with regard to data protection pursuant to Article 43(1) GDPR; 2. has independence and ongoing expertise in relation to the subject matter of assessment pursuant to Article 43(2)(a) GDPR and does not have a conflict of interest pursuant to Article 43(2)(e) of the GDPR; 3. has undertaken to respect the criteria referred to in Article 42(5) of the GDPR, in accordance with Article 43(2)(b) of the GDPR; 4. has relevant and appropriate knowledge and experience in applying data protection legislation ˙ 5. has relevant and appropriate knowledge and experience in technical and organizational data protection measures 6. is able to demonstrate experience in the areas specifically listed in these additional requirements: For personnel with technical expertise: Must have obtained a bachelor's degree in computer science, computer science, or mathematics at least at the LL.P. level 6 from a Greek or foreign university, or equivalent professional education with a recognized title which is recognized by the issuing Member State. The degree from the foreign university must be recognized by the state. In addition, he/she must have obtained a Master's academic degree or equivalent, and have relevant professional experience. Personnel responsible for certification decisions must demonstrate that they have at least two years of professional and comprehensive 14 experience and expertise in identifying and implementing data protection measures.

Personnel responsible for assessments must demonstrate that they have at least two years of professional experience in data protection techniques, as well as knowledge, specialized expertise and professional experience in (e.g. audits and certifications). technical procedures For staff with legal expertise: Must have obtained a law degree from a Greek or foreign university. The foreign university's law degree must be recognized by the state. In addition, he/she must have obtained a Master's degree (LL.M.) or equivalent, and have relevant professional experience. Personnel responsible for certification decisions must demonstrate that they have at least two years of professional and comprehensive experience and expertise in certification measures related to data protection law. Staff responsible for assessments must demonstrate at least two years of professional experience in the field of data protection law as well as knowledge, specialized expertise and professional experience in technical procedures (e.g. audits and certifications). Staff with technical and legal expertise must demonstrate that they maintain sector-specific knowledge of their technical and audit skills through continuous professional development. 6.2 Resources for the assessment The certification body, in addition to the requirements of section 6.2 of the ISO 17065 standard, must demonstrate that the conditions of paragraph 6.1 of those requirements are met for the personnel of the bodies to which the certification body has assigned assessment activities. 7. Procedural requirements, article 43 paragraph 2 items c), d) of the GDPR 7.1 General The E.SY.D., in addition to the requirements of section 7.1 of the ISO 17065 standard, ensures that: 1. certification bodies comply with the additional requirements of the GDPR (in accordance with Article 43 paragraph 1 point b) of the GDPR), so that the duties and obligations do not lead to a conflict of interests in accordance with Article 43 paragraph 2 point b) of the GDPR; 15 2. the competent supervisory authorities have been informed before a certification body starts using an approved European Data Protection Seal in a new Member State through its local office; 3. certification bodies have established procedures to assess that the applicant's processes and mechanisms for processing and managing the of personal data related to the scope of the certification and the subject of assessment comply with the GDPR; 4. the certification bodies have establish procedures/mechanisms so that the APDPH is informed in writing before the granting, extension, renewal or revocation/suspension of the requested certification. The certification body must explain the reasons for the relevant decision to the CAPA and provide a copy of the summary of the evaluation report referred to in section 7.8 (including the following information: the client's name, a description of the certification evaluation object and a brief evaluation accessible from the public); 5. the certification bodies have established procedures to investigate and promptly respond in writing to any requests from the APDPH regarding the provision of aggregated data for the certifications, among others, for submitted

complaints as well as for the provision of detailed data pertaining to a specific case. 7.2 Application In addition to the requirement of section 7.2 of the ISO 17065 standard, the following shall be required: 1. the subject of assessment shall be described in detail in the application. It also includes interfaces and transfers to other systems and organizations, protocols and other safeguards; 2. the request must specify whether processors are used and when the request is made by processors, their responsibilities and tasks must be described, and request to include the relevant contract(s) of the relevant controller/processor; 3. the request must specify whether joint controllers participate in the processing, and when the request is submitted by joint controllers, the responsibilities must be described and their duties, and the application to include the agreed arrangements. During the application stage, the certification body must provide APDPH with a brief description of each of the applications. 16 7.3 Examination of the application In addition to paragraph 7.3 of the ISO 17065 standard, the following must be required: 1. the binding assessment methods regarding the subject of assessment must be specified in the certification agreement; 2. the assessment of paragraphs 7.3.1 item e) and 7.3.3 of ISO 17065 must take into account both technical and legal expertise in the field of data protection, to the extent required; 3. the examination of the application must take into account all the information referred to in paragraph 7.2 of said requirements. 7.4 Evaluation In addition to paragraph 7.4 of the ISO 17065 standard, certification mechanisms must describe adequate assessment methods to assess the compliance of the processing operation(s) with the certification criteria, including areas such as:1. method for assessing the necessity and proportionality of processing operations in relation to their purpose and the relevant subjects of the data; 2. a method to assess the coverage, composition and assessment of all risks that have been considered by the controller and the processor in terms of legal consequences in accordance with Articles 30, 32, 35 and 36 of the GDPR , as well as regarding the determination of technical and organizational measures in accordance with articles 24, 25 and 32 of the GDPR, to the extent that the aforementioned articles are applied to the subject of assessment, and 3. a method for the assessment of corrective measures, including guarantees, of the safeguards and procedures to ensure the protection of personal data in the context of processing, which must be granted to the subject of evaluation, and to demonstrate that the legal requirements set out in the adopted criteria are met and 4. documentation of the methods and of the findings. The certification body should be required to ensure that these assessment methods are standardized and generally applied. This means that comparable assessment methods are used for comparable assessment objects. Any deviation from this procedure must be justified by the certification body. 17 In addition to paragraph 7.4.2 of the ISO 17065 standard, the evaluation must be allowed to be carried out by

external experts recognized by the certification body. The same requirements described in section 6 of said staff requirements apply to said external experts. In addition to paragraph 7.4.5 of the ISO 17065 standard, it must be provided that there is a possibility to include in an applicable certification the existing data protection certification according to articles 42 and 43 of the GDPR, which already covers part of the subject of the certification. However, it is not enough to completely replace (partial) assessments. The certification body is required to check compliance with the criteria in relation to the subject of assessment. For recognition, it is required, in any case, to prepare a complete evaluation report or information that allows the evaluation of the existing certification and its results. A certification statement or similar certification statements should not be considered sufficient in lieu of a report. In addition to paragraph 7.4.6 of ISO 17065, the certification body should be required to specify in its certification scheme in detail how the information required by paragraph 7.4.6 serves to inform the applicant of its irregularities shape. In this context, at least the nature and timing of such information should be specified. In addition to paragraph 7.4.9 of the ISO 17065 standard, it should be required that full access to these documents be provided by the DPA upon request. 7.5 Review In addition to paragraph 7.5 of the ISO 17065 standard, procedures are required for the granting, regular review and revocation of the respective certifications in accordance with Articles 43(2) and 43(3) of the GDPR. In addition to paragraph 7.5.1 of the ISO 17065 standard, the certification body must demonstrate how the person(s) entrusted with the review are not directly or indirectly involved in the assessment process. 7.6 Certification decision In addition to paragraph 7.6.1 of the ISO 17065 standard, the certification body should be required to specify in detail in its procedures how its independence and responsibility for individual certification decisions are ensured. The certification body must inform the APDPH in writing before issuing the certification decision and state the reasons for the relevant decision. 18 In addition to paragraph 7.6.6 of the ISO 17065 standard, the certification body must state the place, manner and deadline for the applicant to appeal against the certification body's decision not to grant certification or to request its review. 7.7 Certification documentation In addition to paragraph 7.7.1.e of the ISO 17065 standard and in accordance with article 42 paragraph 7 of the GDPR, it must be required that the validity period of certifications does not exceed three years. In addition to paragraph 7.7.1.e of the ISO 17065 standard, documentation of the intended monitoring period within the meaning of section 7.9 of those requirements shall also be required. In addition to paragraph 7.7.1.f of the ISO 17065 standard, the certification body should be required to state the subject of assessment in the certification documentation (stating the issue status or similar characteristics, as appropriate). 7.8 Index of certified products In addition to paragraph 7.8 of the ISO 17065 standard, the

certification body should be required to keep information about certified products, processes and services accessible internally and to the public. The certification body provides the public with a summary of the evaluation report. The aim of this summary is to contribute to transparency around what has been certified and how it has been assessed. It includes the following: a) the customer's name and contact details, b) the scope of certification and a substantial description of the evaluation object, c) the corresponding certification criteria (including version or functional status), d) the evaluation methods and the tests conducted, e) the result(s), f) the date of grant and expiration date of the applicable certification, and g) the dates of initial certification and re-certification. In addition to paragraph 7.8 of the ISO 17065 standard and in accordance with article 43 paragraph 5 of the GDPR, the certification body informs the APDPH of the reasons for granting or withdrawing the requested certification. 19 7.9 Monitoring In addition to paragraphs 7.9.1, 7.9.2 and 7.9.3 of the ISO 17065 standard, and in accordance with Article 43(2)(c) GDPR, regular monitoring measures are required to maintain certification during of the monitoring period. These measures should be risk-based and proportionate, and surveillance activities should be carried out at least twice during the certification period. The type and frequency of supervision activities should be specified in the certification scheme. 7.10 Changes affecting certification In addition to ISO 17065 clauses 7.10.1 and 7.10.2, changes affecting certification that are taken into account by the certification body include: amendments to data protection legislation, delegated acts of the European Commission in accordance with Article 43 paragraphs 8 and 9 of the GDPR, decisions and documents issued by the EDPS and judicial decisions regarding data protection. The above changes also include the case where the latest developments in technology, which were valid at the time of certification and which were taken into account for its granting, have now become obsolete due to recent developments in technology. The amendment procedures to be carried out by the certification body must include the following: transitional periods, approval process by the FSA, re-evaluation of the relevant subject of the certification and appropriate measures to revoke the certification if the certified processing operation no longer meets the updated Criteria. 7.11 Termination, restriction, suspension or revocation of certification In addition to paragraph 7.11.1 of the ISO 17065 standard, the certification body must be obliged to inform immediately and in writing the APDPH and the E.SY.D. on the measures taken and on the continuation, limitations, suspension and revocation of certification. Additionally, in cases where the certification body finds non-compliance, it must specify in its requirements what measures should be taken. According to article 58 paragraph 2 point h) of the GDPR, the certification body must accept the decisions and orders of the APDPH to revoke or not grant certification to a client (applicant), if the certification requirements are not met or have ceased to be met. In

corresponding 20 cases, the certification body must provide the APDPH with clear and documented evidence proving that the appropriate measures have been taken. Serious incidents of personal data breaches related to the scope of certification and the subject of assessment should be considered non-compliance with the certification and appropriate actions should be taken by the certification body. For these actions, the certification body must immediately inform the APDPH in writing.Hthis requirement does not affect the customer's obligation to inform the APDPH
regarding incidents of data breach in accordance with the provisions of the GDPR.

7.12 Files

The certification body should be required to keep all documents complete,
comprehensible, up-to-date and suitable for control.

In addition to clauses 7.10 and 7.12 of ISO 17065, the certification body
must keep a record of all changes affecting certification, measures
taken to make the changes and its status
certification.

The details of the persons of the certification body responsible for the
assessment and certification decision must be kept on file
separately for each certification case and to be available to APDPH
if requested. The purpose of this requirement is for the APDPH to have the possibility,
when deemed appropriate, verify that the personnel responsible for the
evaluations are different from the personnel responsible for the decisions
certification for each certification case (ie segregation of duties).

7.13 Complaints and appeals, Article 43(2)(d) GDPR

In addition to paragraph 7.13.1 of the ISO 17065 standard, it shall be required by
the certification body to determine

a) who can submit complaints or objections,

b) who processes them on the part of the certification body,

c) what verifications are carried out in this context, and

d) the possibilities of consultation with interested parties.

In addition to paragraph 7.13.2 of the ISO 17065 standard, it should be required

by the certification body to determine

a) in what way and to whom this confirmation must be given,

b) what are the relevant deadlines, and

c) what processes are started next.

21

In addition to paragraphs 7.13.7 and 7.13.8 of ISO 17065, the body

certification must be required to set reasonable time limits for the correct

informing interested parties who have filed complaints about

progress, outcome and termination of the complaints process.

In addition to paragraph 7.13.1 of the ISO 17065 standard, the certification body

must determine the manner in which the separation between the

certification activities and the handling of appeals and

complaints.

Certification bodies must publish their handling procedure

complaints and make it easily accessible to the public.

8. Management System Requirements

A general requirement for the management system according to chapter 8 of

standard ISO 17065 is that the implementation of all the requirements from the previous ones

funds in the scope of the certification mechanism by the accredited

certification body must be documented, evaluated, audited and

monitored independently.

The basic principle of management is to define a system according to

whose objectives are set effectively and efficiently, and

namely: the implementation of certification services through appropriate

specifications. This requires transparency and verifiability of their application

accreditation requirements from the certification body and its ongoing compliance.

For this purpose, the management system must define a methodology

for the satisfaction and control of these requirements in accordance with

regulations for data protection and for lasting

their verification by the accredited body itself.

These management principles and their documented application must be

transparent and disclosed by the accredited certification body based

of the accreditation process and in accordance with article 58 of the GDPR and at

continued at the request of the APDPH at any time during an investigation

in the form of data protection checks in accordance with Article 58

paragraph 1 point b) of the GDPR or review of the certifications that

are issued in accordance with article 42 paragraph 7 of the GDPR, according to article 58

paragraph 1 point c) of the GDPR.

In particular, the accredited certification body must make public

permanently and continuously the certifications it issued and the basis (or mechanisms

or the certification systems) used to grant them, the timeline

period of validity of the certifications, the framework and the conditions under which

apply (recital 100 GDPR).

9. Further Supplemental Requirements

9.1 Update of evaluation methods

The certification body must establish procedures to guide it

updating the evaluation methods applied in its context

evaluation of paragraph 7.4 of said requirements. The update should

to be carried out in the context of changes in the legal framework, of the relevant

of risk/s, as well as the development of technology and implementation costs

of technical and organizational measures.

9.2 Retention of Expertise

Certification bodies must establish procedures to ensure it

training of their employees in order to update their skills,

taking into account the developments mentioned in paragraph 9.1 of the said

requirements.

9.3 Responsibilities and Responsibilities

9.3.1 Communication between the certification body and applicants and clients

of

Procedures must be in place to implement appropriate procedures and

communication structures between the certification body and applicants and clients

of. These include the following:

1. Maintain documentation of duties and responsibilities from

the accredited certification body, in order to:

a) information requests, or

b) the possibility of contact in the event of a complaint regarding the

certification.

2. Maintaining an application process for the purpose of:

a) information on the progress of the application;

b) assessments of the APDPH in relation to

i. comments;

ii. decisions of the APDPH.

9.3.3 Managing Complaints Handling

The complaints handling process should be an integral part of it

management system, which applies in particular the requirements of the paragraph

4.1.2.2 points c) and j), of paragraph 4.6 point d) and paragraph 7.13

of the ISO 17065 standard.

The relevant complaints and objections must be communicated to the APDPH.

23

9.3.4 Management of withdrawal

Procedures in case of suspension or revocation of accreditation must

are integrated

of

certification,

including notifications to customers.

management

system

carrier

in the

24

Title: Supplementary requirements of the Authority for the accreditation of bodies

certification incorporating the recommendations of the relevant opinion 22/2020 of

European Data Protection Board

Summary: The Authority, with its decision number 25/2020, decided unanimously,

amending the draft supplementary requirements for accreditation

of the certification bodies, based on the recommendations and encouragements of the relevant

opinion 22/2020 of the European Data Protection Board and

communication of the amended plan to the Council. The original plan, as it was

formed by the Authority's Decision No. 8/2020, had been submitted to

Council under the Cohesion Mechanism

of the GDPR. The

amended supplementary requirements will be published by the Authority at its website after the completion of said process.