

NATIONAL DATA PROTECTION COMMISSION

Regulation No. 834/2021

Summary: Additional accreditation requirements for certification bodies.

In accordance with subparagraph p) of paragraph 1 of article 57, as well as subparagraph b) of paragraph 1 of article 43 and paragraph 3 of article 43 of the General Regulation on Data Protection (1), hereinafter referred to as RGPD, it is up to the National Data Protection Commission (CNPd) to set the requirements additional accreditation against ISO/IEC 17065/2012.

Pursuant to the provisions of subparagraph e) of paragraph 1 of article 6 of Law n.º 58/2019, of 8 August (2), the CNPD, as the national data protection control authority, and the Portuguese Institute of Accreditation, I.P. (IPAC), as a national accreditation body, established through protocol the terms of cooperation and articulation between the two institutions within the scope of the accreditation requirements (3).

This regulation defines the additional accreditation requirements, presented, in its structure and numbering, in accordance with the corresponding sections of ISO/IEC 17065/2012.

In this way, the requirements relating to data protection are specified in each point or section. personal data, also highlighting the situations in which additional requirements are not imposed on the defined in ISO/IEC 17065/2012.

In the elaboration of the additional accreditation requirements, the guidelines of the European Data Protection Board regarding the implementation of accreditation and certification processing of personal data (4).

There was no public consultation, as this regulation essentially reflects the

guidelines approved by the European Data Protection Committee on this matter, which have already been the subject of public consultation, and the content of which, as well as the opinion issued by the same Committee on the draft regulation, the CNPD is legally bound.

Additional accreditation requirements are binding and may be subject to review and update when necessary.

Thus, under the provisions of subparagraph b) of paragraph 1 of article 43, paragraph 3 of article 43 and Article 57(1)(p) of the GDPR, the CNPD determines the following additional requirements of accreditation in relation to ISO/IEC 17065/2012:

1 — Purpose and scope

The scope of application of ISO/IEC 17065/2012 (hereinafter, ISO/IEC 17065), which covers pipelines, processes and services, is broader than the scope of certification regulated by the GDPR, by whereas, for the purpose of applying this Regulation, ISO/IEC 17065 must be applied in compliance therewith.

Certification under the GDPR must cover the processing of personal data, being only applicable to data processing operations carried out by those responsible and subcontractors in accordance with Article 42(1) of the GDPR.

2 — Normative references

This regulation has as normative references the following legal acts:

GDPR;

Law No. 58/2019, of August 8;

DRC001 (General Accreditation Regulation), published by IPAC, and documents differentiated.

The GDPR takes precedence over ISO/IEC 17065. Whenever, in the additional requirements or in the certification procedure, if reference is made to the requirements of ISO/IEC 17065, the same be interpreted in accordance with the GDPR.

September 6, 2021

PART B

page 16

3 — Terms and definitions

The terms and definitions of ISO/IEC 17065 are adopted whenever they do not differ from the terms and GDPR definitions as interpreted by the European Data Protection Board in its guidelines on accreditation and certification (5), which are reproduced here.

4 — General requirements

4.1 — Legal and contractual aspects

4.1.1 — The certification body must be able to demonstrate, at all times, to IPAC, which has updated procedures capable of proving compliance with the legal responsibilities defined under the terms of accreditation, including additional requirements concerning the application of the GDPR. Furthermore, he must be able to demonstrate that he has GDPR-compliant procedures and specific measures to process the personal data of applicants and customers (6), within the scope of the certification process.

In particular, you must inform if you are aware that you are being investigated by the CNPD and if you have been convicted of violating the legal data protection regime in the last 4 (four) years. Regardless of the fulfillment of this duty, IPAC may consult the CNPD to obtain the information required within the framework of the accreditation procedure.

The accreditation procedure may be impaired if there has been a violation of the GDPR and sanctioning decision issued by the CNPD, justifying the suspension of the procedure, until the applicant demonstrates the adoption of the necessary measures to correct that violation.

4.1.2 — The certification body must demonstrate that its certification contract:

a) Requires that the applicant also meets the certification criteria approved by the CNPD or by the European Data Protection Board (7);

b) Requires the applicant to guarantee full transparency before the CNPD within the scope of the procedure.

certification process, in particular access to information necessary to verify compliance

by the data protection regime, including information covered by contractual clauses of

confidentiality relating to compliance with the data protection regime (8);

c) Requires the applicant to guarantee access for the purpose of carrying out testimonies and visits

control by IPAC;

d) Does not diminish the applicant's responsibility in complying with the

personal data and does not affect the attributions and powers of the CNPD;

e) Requires the applicant to guarantee the certification body access to its activities

of treatment and all the information necessary for the processing and conclusion of the procedure

certification (9);

f) Requires the applicant to observe the applicable deadlines and procedures, namely

those arising from the certification mechanism;

g) Specifies the rules for validity, renewal and withdrawal of certification, including the definition

setting appropriate intervals for reassessment or review (10);

h) It legitimizes the certification body to make available to the CNPD all information concerning

the reasons for granting the certification, as well as providing the necessary elements

to the public register of certification procedures by the European Committee for the Protection of

Data (11);

i) Includes rules on the investigation of complaints, binding the customer to guarantee the trans-

parency and access to complaints management rules and procedures (12);

j) Explain the consequences of the withdrawal or suspension of accreditation for the

certification, including possible impact and consequences for the customer and the measures that may

be subsequently adopted;

k) Requires the applicant to inform, as soon as he becomes aware of it, the certification body

of the occurrence of situations of non-compliance with the RGPD and other protection legislation

applicable data, declared by the CNPD or the Courts, or other protection certification

data that may affect the required certification, as well as any changes to the products,

processes or services to which the certification relates;

l) Defines the binding assessment methods as to the object of the certification.

Diário da República, 2nd series

No. 173

September 6, 2021

PART B

page 17

4.1.3 — The certification body may only use certificates, marks and seals that comply

the provisions of articles 42 and 43 of the GDPR and in the guidelines on accreditation and certification

by the European Data Protection Board (13).

4.2 — Management of impartiality

The certification body must demonstrate, to the satisfaction of the CNPD, that it is

dependent on the organization applying for certification, as required in subparagraph a) of paragraph 2 of the

Article 43 of the GDPR.

In particular, it must be able to demonstrate that neither the certification body,

nor the persons who are authorized to make decisions or the workers who intervene in the

certification procedure, have personal links with the applicant/client. the organism of

certification must also demonstrate that it has no share in the applicant/client nor is

co-financed by him, nor financed by him; likewise, it cannot integrate companies of the same

corporate group of the applicant/client.

It is also up to the certification body to demonstrate that there is no economic relationship

between him and the applicant/client, in particular a subcontracting relationship for treatment of

personal data.

The certification body must demonstrate, to the satisfaction of the CNPD, that its

functions and obligations do not imply a conflict of interest, as required in subparagraph e) of Article 43(2) of the GDPR.

For this purpose, it must create procedures that allow detecting and analyzing the risk of conflict of interests arising from activities or relationships of the certification body itself and its personnel, defining clear rules that prevent conflicts. For example, ensuring that you always that one of your workers is also providing services to the applicant/client that declare and, consequently, be removed from the concrete certification procedure. In addition, it must establish clear rules on the management of conflict of interests situations. specifically identified.

4.3 — Legal liability and financing

IPAC must regularly ensure that the certification body has adopted appropriate guarantee measures for its liabilities (e.g. insurance or reserve fund) in the regions geographical areas in which it operates.

4.4 — Non-discriminatory conditions

No additional requirements.

4.5 — Confidentiality

No additional requirements.

4.6 — Publicly accessible information

The certification body must have publicly accessible:

- a) All versions of the certification criteria (both current and previous) approved by the CNPD in accordance with paragraph 5 of article 42 of the RGPD, as well as all procedures for certification, indicating the respective period of validity;
- b) Information on the procedure for analyzing complaints and appeals, as per subparagraph d) of Article 43(2) of the GDPR.

If the certification body makes an electronic site available, the information

ISO/IEC 17065 or this regulation require it to be publicly available

will be accessible on that site, with an exposure at least equal to that used to advertise

or list your services.

5 — Structural requirements

5.1 — Organizational structure and top management

The certification body must inform the CNPD and IPAC in advance if it wishes to initiate or develop activities from a branch, delegation or other legal representation installed in another country.

5.2 — Mechanism to safeguard impartiality

No additional requirements.

Diário da República, 2nd series

No. 173

September 6, 2021

6 — Resource requirements

6.1 — Certification body personnel

a) The certification body must demonstrate that its personnel:

PART B

page 18

i) enjoys independence and impartiality in relation to the organization being evaluated,

in accordance with points a) and e) of paragraph 2 of article 43 of the GDPR;

ii) It complies with the criteria set out in paragraph 5 of article 42 and in paragraph b) of paragraph 2 of article 43. of the GDPR;

iii) Demonstrates ongoing expertise (knowledge and experience) in data protection, in accordance with Article 43(1) of the GDPR, including the following minimum competencies but:

(a) Adequate and relevant knowledge and experience in the application of the legal regime of data protection;

(b) Adequate and relevant knowledge and experience with technical and organizational measures

data protection measures, where relevant.

b) The certification body must demonstrate that those responsible for managing the processes

certification bodies (including those who plan audits and appoint audit teams) have:

i) Adequate and relevant knowledge of procedures and certification criteria in

ii) Knowledge of procedures and methods of assessment in terms of the protection of

data protection matters;

Dice;

c) The certification body shall demonstrate that those responsible for certification decisions

certification (i.e., who analyzes the assessment reports, assesses and decides on non-conformities

and decides on the granting, extension, renewal, suspension and withdrawal of certification) have the

following minimum skills:

i) Regarding people with technical expertise:

(a) Knowledge and expertise gained from a degree in computer science or other

equivalent scientific area (EQF level 6) (14), or a professionally recognized title in

relevant field, or significant professional experience;

(b) Relevant professional experience in identifying and applying data protection measures

technical and organizational data;

(c) Knowledge of ISO/IEC 17065 and additional accreditation requirements;

ii) Regarding persons with legal specialization:

(a) Knowledge obtained in a degree in law (EQF level 6) of at least eight

semesters, or a master's degree or equivalent, or significant work experience;

(b) Relevant professional experience regarding data protection legislation;

(c) Knowledge of ISO/IEC 17065 and additional accreditation requirements.

d) The certification body must demonstrate that those responsible for the assessments have

the following minimum skills:

i) Regarding people with technical expertise:

(a) Knowledge and expertise gained from a degree in computer science or other equivalent scientific field (EQF level 6), or a professionally recognized title in a field relevant, or significant work experience;

(b) Professional experience of at least 2 (two) years in the technological aspect of protection of data;

Diário da República, 2nd series

No. 173

September 6, 2021

PART B

page 19

(c) Knowledge of ISO/IEC 17065 and additional accreditation requirements;

(d) Knowledge and relevant professional experience in equivalent procedures (e.g., certification and audit);

ii) Regarding persons with legal specialization:

(a) Knowledge obtained in a degree in law (EQF level 6) of at least eight semesters, or a master's degree or equivalent, or significant work experience;

(b) Relevant professional experience of at least 2 (two) years regarding the legislation of

(c) Knowledge of ISO/IEC 17065 and additional accreditation requirements;

(d) Knowledge and relevant professional experience in equivalent procedures (e.g., data protection; certification and audit).

e) The certification body shall define procedures that ensure and demonstrate that your staff periodically update their knowledge of personal data protection, taking into account, inter alia, legislative changes, technological developments and their impact the risks to data protection and privacy, as well as their knowledge of

technical and auditing skills, when applicable.

6.2 — Resources for the evaluation

No additional requirements.

7 — Procedural requirements

7.1 — General

In the procedures referred to in points c) and d) of paragraph 2 of article 43 of the GDPR, the body certification must comply with additional accreditation requirements, in particular in order to ensure ensure that its attributions and obligations do not imply a conflict of interest (15).

In defining the certification criteria, the certification body shall:

- a) Take into account the guidelines approved by the European Data Protection Board (16);
- b) Require approval of the certification criteria by the CNPD before being accredited, and want new approval by the CNPD whenever it changes, in substantive terms, the aforementioned criteria.

In case the certification body intends to act in other Member States, notify and, if necessary, obtain approval from the corresponding competent authorities, including for the use of tion of a European Data Protection Seal, in accordance with Article 42(5) of the GDPR.

The certification body shall also investigate the client for violations of the data protection law whenever the customer informs him that he is being of an investigation process, related to the scope and object of the certification, by the CNPD or if this entity notifies you of this fact.

It must also cooperate with the CNPD in ongoing investigations on the clients it has certified; the certification body must provide the CNPD with an appraisal report on the investment. made, concluding if the client still meets the conditions to be certified.

Furthermore, the certification body must keep documentation of its activity (relative to to their functions and obligations), in the event of receiving requests for information or to to allow contact in the event of a claim concerning a certification. In addition, they must procedural mechanisms of communication between the certification body and the

client, to speed up the processing and response to requests for information about the procedure in course or other pertinent information, and that allow eventual appreciation by the CNPD of the their responses and decisions.

7.2 — Candidacy

The certification body shall require the certification application to identify:

a) The intended scope of certification, with a complete description of the certification object, including any interfaces, communications to other systems or organizations, protocols and other binding provisions relating to the subject of certification;

Diário da República, 2nd series

No. 173

September 6, 2021

PART B

page 20

b) The existence of subcontracting of data processing and, when the applicant is subcontracted, contractor, its functions and obligations, and in both cases a copy must be submitted the subcontracting contract;

c) The existence of joint liability, in which case a copy of the agreement between jointly responsible persons; and

d) Any inquiries or investigations related to the scope and object of the certificate cation, made by the CNPD to the applicant, current or occurred since May 25, 2018.

The certification body must electronically notify the CNPD and IPAC of the applicants. ments, also for the purpose of verifying the existence of investigations in progress or eventual sanctioning decisions of the CNPD; those public entities ensure the of the procedures, being able to monitor the activities of the certification body.

7.3 — Analysis of the application

In planning and carrying out the assessment, the certification body shall include both the

technological aspect, or the legal aspect of data protection.

7.4 — Assessment

a) The certification body shall sufficiently and comprehensively establish the methods of assessment to use to determine the compliance of the certification object with the criteria of certification and the legal data protection regime. In particular and where applicable, you must discriminate:

- i) The method(s) to assess the necessity and proportionality of processing operations of data in relation to the stated purpose or purposes and the data collected, also taking into account the universe of data subjects;
- ii) The method(s) to consider the scope, nature and assessment of the risks identified ceded and considered by the person in charge or by the subcontractor, in relation to the consequences legal provisions provided for in articles 30, 32, 35 and 36 of the GDPR, and the corresponding technical measures and organizational arrangements adopted pursuant to Articles 24, 25 and 32 of the GDPR, insofar as such articles apply to the object of certification;
- iii) The method(s) for evaluating corrective measures, including guarantees, safeguards and provisions to ensure the protection of personal data in the context of data processing covered by the object of certification, and to demonstrate that such measures are in compliance with the legal regime of data protection and, especially, with the constant requirements of the certification criteria;
- iv) Documents supporting the procedures and the model document for registration verifications and assessment of compliance with certification criteria and the protection regime of personal data.

b) The certification body shall use standardized assessment and application methods. tion for similar certification objects (17). Any deviation from this procedure must be substantiated by the certification body.

c) The certification body shall periodically review its assessment methods,

including the corresponding procedures, in the face of changes in the legal or legal framework, when development of new technologies, the relevant risks, the state of the art and the costs of implementation of technical and organizational measures.

d) The certification body shall establish the conditions and procedure for using information on any certification previously obtained in accordance with articles 42 and 43 of the GDPR that the customer wishes to see recognized or taken into account. Note that the body of certification should be required to assess in detail that certification for compliance with the relevant certification criteria. In any case, this depends on the availability of a report complete assessment or information about the assessment of the previous certification activity and of the respective results.

e) The certification body must document the duration methodology in a procedure of assessments (rater/day), which must be proportional to the universe and nature of the data

Diário da República, 2nd series

No. 173

September 6, 2021

PART B

page 21

included in the scope of certification, to the universe of data subjects, to the context of the treatment, the complexity of the technologies used in the collection and subsequent treatment of the themselves, and the use of subcontracting by the customer.

f) The certification body may carry out its assessment tasks through own staff or external experts hired for this purpose, without prejudice to the use of the contracting the provision of services as defined in ISO/IEC 17065. In any case, the certification body is responsible for the decision taken.

g) The evaluation reports must identify the documents and records examined, pro-evaluated processes, functions performed by the people interviewed, as well as any

non-conformities in relation to the certification criteria, clearly identifying the requirement

breached and the seriousness of the breach.

h) After the issuance of the certification, in the context of monitoring by the certification body,

notification, any non-conformities detected must be corrected by the customer within a period

proportional to its severity. To this end, the certification body must typify the

compliances depending on their severity — in less serious cases, the deadline can reach

one month, after which, in the absence of correction, the process of suspension of the

certification. In the most serious cases, in addition to correction, the certification body must request

the customer an analysis of the causes of non-compliance, so that (i) implement corrective actions

effective measures that prevent its recurrence, and (ii) can determine whether there are other related failures.

nothing or similar to the one detected and that must also be corrected.

i) Whenever the CNPD so requests, the certification body guarantees access to the entire

documentation relating to the assessment.

7.5 — Review

Pursuant to paragraphs 2 and 3 of article 43 of the GDPR, procedures must be established

for the issuance, periodic review and withdrawal of certification. In certification procedures,

including those referring to the periodic review and withdrawal of certification, the reasons for the decision

must be clearly identified and documented, with objective facts and evidence, regardless of

mind of whoever does it.

7.6 — Certification decision

The certification body must specifically define how its

independence and responsibility for individual certification decisions.

To ensure transparency, you should also have procedures in place to notify

the CNPD prior to a decision on certification, renewal or extension of the

same. The notification includes a summary of the activities carried out to reach the decision, including

a copy of the audit report, of the review process, as well as the reasons for the decision,

second model to be established by the CNPD. In the case of concession, extension and renewal, you must jointly submit the draft certificate of conformity or documentation that replaces it.

The certification body shall further confirm, immediately prior to the decision, if the customer is not subject to investigations by the CNPD that may jeopardize the pre-certification tended.

7.7 — Certification documentation

According to paragraph 7 of article 42 of the GDPR, the certification cannot have a longer validity

The monitoring period referred to in point 7.9 must be documented. of
to 3 (three) years.

this Regulation.

The description of the scope of certification must include the identification of the certification object, the entity covered by the certification, as well as the identification and version of the certification criteria cation applied.

The certification body must send the CNPD a copy of the marks or seals used.

7.8 — Directory of certified products

The certification body shall make publicly available information relating to the certified products, processes and services. If the certification body has a site on the Internet, you must make available the directory related to the certifications issued there.

Diário da República, 2nd series

No. 173

September 6, 2021

PART B

page 22

In particular, it must publish an executive summary which sets out the scope and object of the certification, its period of validity, conditions to which certification is subject, as well as a summary of the certification criteria applied, the evaluation methods adopted and the

results obtained.

It must also inform, electronically, the CNPD about the grounds for granting the certification, as well as its withdrawal (18).

7.9 — Follow-up

The certification body shall establish in a proportionate and non-discriminatory manner the periodic assessment mechanisms during the period of validity of the certification (19).

The certification body shall establish the conditions and procedure for using information on any certification previously obtained in accordance with articles 42 and 43 of the GDPR that the customer wishes to see recognized or taken into account.

Monitoring activities must be carried out on an annual basis, and the first activity exceeds 12 months after the date of the assessment carried out for the purpose of the concession certification, without prejudice to its completion in a shorter period of time whenever the result of a risk analysis justifies it.

7.10 — Changes that affect certification

Changes affecting certification, to be considered by the certification body, include:

- a) Notifications of personal data breaches related to the scope and object of the certification or non-compliance, declared by the CNPD or the Courts, the GDPR or the requirements additional;
- b) Legislative changes on data protection;
- c) Adoption of delegated or implementing acts by the European Commission in matters of protection data (20);
- d) Relevant documents adopted by the European Data Protection Board;
- e) Court decisions on data protection;
- f) Changes in the state of the art.

To that end, it should provide for amendment procedures that include transitional periods,

submission of an application for approval to the CNPD, reassessment of the certification object and eventual de-certification measures.

7.11 — Annulment, reduction, suspension or withdrawal of certification

In the event of revocation, reduction, suspension or withdrawal of certification, the certification body must notify the client of the decision and its grounds, as well as inform immediately the CNPD, including the reasons for such decision, without prejudice to its communication to IPAC.

The certification body shall establish proportionate sanctions in case of failure, concealment or delay in the communication, by the customer, of information regarding the investigations in progress or non-compliance with the legal data protection regime.

If the CNPD understands that the certification criteria are not or are no longer being met, may order the certification body, under the terms of subparagraph h) of paragraph 2 of article 58. of the RGPD, which does not issue or withdraw a certification, which is constituted in the duty of its immediate compliance.

7.12 — Records

The certification body must retain complete, comprehensible, updated and auditable.

7.13 — Complaints and appeals

The certification body shall establish and make available grievance procedures and appeal, in particular, rules on legitimacy, instruction and consultation by interested parties, as well as such as adequate response times and proportionate to the severity and scope of complaints and resources, ensuring independence in their analysis. It must also define the processes to be adopt after the decision on the complaint or appeal has been issued, namely, transmitting to the CNPD the relevant complaints and appeals.

Diário da República, 2nd series

No. 173

September 6, 2021

In addition, the certification body must establish rules that guarantee the effective se-
between certification activities and the processing of complaints and appeals.

8 — Management system

Whenever this Regulation provides for or refers to the obligations of the
certification, the procedure and methodology adopted for its compliance must be
documented in the respective management system, in order to allow the effective and efficient pursuit of
of the objectives pursued, as well as the transparency and auditability of the application and compliance with the
additional requirements.

The certification body must also provide the CNPD with the management principles and their
documented application, during and after the accreditation procedure, whenever this entity
requests it, at any time, during an investigation within the scope of the powers conferred by the
Article 58 of the GDPR.

(1) General Data Protection Regulation, approved by Regulation (EU) 2016/679 of the European Parliament
peu and of the Council of 27 April 2016 on the protection of natural persons with regard to processing
of personal data and the free movement of such data.

(2) Ensuring the implementation, in the national legal system, of Regulation (EU) 2016/679 of the European Parliament
and of the Council of 27 April 2016.

(3) The protocol between the CNPD and IPAC, IP, is available on the websites of both entities.

(4) Guidelines 4/2018 of the European Data Protection Board, concerning the accreditation of data protection bodies
certification pursuant to article 43 of the General Data Protection Regulation (2016/679), version 3.0, of 4 December
June 2019, accessible at [https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201804_v3.0_accre-
dictationcertificationbodies_annex1_en.pdf](https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201804_v3.0_accre-
dictationcertificationbodies_annex1_en.pdf) and Guidelines 1/2018 of the European Data Protection Board, concerning the
certification and the definition of certification criteria in accordance with articles 42 and 42 of the GDPR, version 3.0, of
4 June 2019, accessible at https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201801_v3.0_cer-

tificationcriteria_annex2_pt.pdf

(5) Guidelines 4/2018 of the European Data Protection Board., concerning the accreditation of data protection bodies. certification pursuant to article 43 of the General Data Protection Regulation (2016/679), version 3.0, of 4 December June 2019, accessible at https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201804_v3.0_accreditationcertificationbodies_annex1_en.pdf and Guidelines 1/2018 of the European Data Protection Board, concerning the certification and the definition of certification criteria in accordance with articles 42 and 42 of the GDPR, version 3.0, of 4 June 2019, accessible at https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201801_v3.0_certificationcriteria_annex2_pt.pdf

(6) In ISO/IEC 17065, the term “client” is used interchangeably, regardless of whether or not the certification has been issued. In view of point 3 of these Regulations, the term "applicant" is used in its literal sense whenever that the certification has not yet been issued and the term “client” when the organization already holds the certification.

(7) In accordance with Article 43(2)(b) and Article 42(5) GDPR.

(8) In order to ensure the application of the provisions of Article 42(7) and Article 58(1)(c) of the

(9) In accordance with Article 62(6) of the GDPR.

(10) Pursuant to Article 43(5) and Article 42(8) of the GDPR.

(11) Pursuant to Article 43(5) and Article 42(8) of the GDPR.

(12) Pursuant to Article 43(5) and Article 42(8) of the GDPR.

(13) Guidelines 1/2018 of the European Data Protection Board on certification and definition of criteria certification in accordance with articles 42 and 42 of the GDPR, version 3.0, of 4 June 2019, accessible at https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201801_v3.0_certificationcriteria_annex2_en.pdf

(14) Cf. <https://ec.europa.eu/ploteus/en/compare?>

(15) Pursuant to Article 43(2)(b) and (e) of the GDPR.

(16) Guidelines 1/2018 of the European Data Protection Board, concerning certification and the definition of criteria certification in accordance with articles 42 and 42 of the GDPR, version 3.0, of 4 June 2019, accessible at https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201801_v3.0_certificationcriteria_annex2_en.pdf

(17) Guidelines 4/2018 of the European Data Protection Board., concerning the accreditation of data protection bodies.

certification pursuant to article 43 of the General Data Protection Regulation (2016/679), version 3.0, of 4 December June 2019, accessible at https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201804_v3.0_accreditationcertificationbodies_annex1_en.pdf

(18) In accordance with Article 43(5) of the GDPR.

(19) In accordance with Article 43(2)(c) of the GDPR.

(20) Pursuant to Article 43(8) and (9) of the GDPR.

GDPR

April 14, 2021. — The President of the National Data Protection Commission, Filipa

Calvão.

314525693

www.dre.pt