CERTIFICATION SCHEME FOR DATA PROTECTION DELEGATES OF THE SPANISH PROTECTION AGENCY OF DATA (AEPD-DPD SCHEME)

CERTIFICATION SCHEME FOR DATA PROTECTION DELEGATES OF THE SPANISH PROTECTION AGENCY OF DATA (AEPD-DPD SCHEME)

Drafted by the Certification Area of the Spanish Agency for Data Protection
December 23, 2019. Version 1.4

Index

1. OBJECT

The purpose of this document is to establish the conditions and requirements that make up and regulate the operation of the Personnel Certification Scheme for the category of "Data Protection Delegate" (hereinafter, AEPD - DPD Scheme, or the Scheme), included in Section 4 of Chapter IV of Regulation (EU) 2016/679, of the European Parliament and of the Council of April 27, 2016, regarding the protection of natural persons with regard to the processing of personal data and the free movement of these data, and the interrelationships between the different Agents that are involved in said certification under accreditation conditions.

The certification of persons is an adequate and valid tool for the objective and impartial evaluation of the competence of an individual to carry out a certain activity. The subsequent public declaration made by the certifier provides the market with useful and verified information on the criteria applied and the requirements demanded of people to obtain professional certification. The validity and validity of the Scheme rules is ensured through the active involvement of experts and representatives of the different interested parties in its development.

The technical competence of the certification entities involved and their alignment with the requirements set by the Scheme, as well as their systematic and impartial performance, are achieved through their accreditation by the National Accreditation Entity (hereinafter, ENAC), in accordance with the requirements of international standards for the certification of persons.

The Spanish Agency for Data Protection (hereinafter, AEPD, or the Agency), as the owner of the Scheme, is responsible for its development and review, actively involving the different interested parties in both processes through a Committee. Technical, subject to an operating Regulation, which ensures both the equitable representation of all the parties involved and the periodic meeting for the analysis and evaluation of the work and tasks of the DPO and its coherence with the competence requirements and the mechanisms for your evaluation.

The AEPD defines, through the aforementioned Committee, the criteria for the recognition of the entities that can carry out the conformity assessment (certification), aimed at enabling the granting of the "Mark of Conformity" associated with the APD - DPD Scheme promoted by it. , which uniquely and unequivocally identifies those people who have demonstrated their competence to carry out the tasks of the DPO.

1.1 REFERENCES

- UNE-EN ISO / IEC 17024: 2012. Conformity Assessment. General requirements for the organizations that carry out the certification of persons.
- Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016, regarding the protection of natural persons with regard to the processing of personal data and the free circulation of these data, by which it is repealed Directive 95/46 / CE (General Data Protection Regulation).
- Organic Law 3/2018, of December 5, on the protection of personal data and guarantee of digital rights.

All the documents cited are applicable in their latest valid edition.

1.2 ACRONYMS

- DPD: Data Protection Delegate.
- AEPD-DPD Scheme: AEPD DPD Certification Scheme.
- RGPD: General data protection regulation.
- LOPDPGDD: Organic Law on the protection of personal data and guarantee of digital rights.

2 SCHEME AGENTS

- **The Spanish Agency for Data Protection (AEPD).** Owner of the Scheme, is responsible for promoting its development, review and continuous validation and authorizes the rest of the agents to be an active part of it.
- **The National Accreditation Entity (ENAC).** Designated by the AEPD as the sole body for the accreditation of certification entities that wish to participate in the Scheme, bearing in mind both the requirements of the UNE-EN ISO / IEC 17024: 2012 standard, as well as the specific requirements defined by the Scheme.
- **The Certification Entities (EC).** They offer certification, exclusively under ENAC accreditation and in accordance with the requirements of the Scheme and the UNE-EN ISO / IEC 17024: 2012 standard, for the category of “Data Protection Delegate”. As part of the process, they may receive rights of use and rights to license the use of the "Mark of Conformity" to Training Entities and certified persons, in the terms established in Annex II.

- **The Training Entities (EF).** They are the entities that offer the appropriate training to satisfy the prerequisites of the certification in this regard. The AEPD may establish, where appropriate, a public and non-discriminatory process for the authorization of EF.

3 MARK OF THE SCHEME

The AEPD, in order for the market to identify the Data Protection Delegates certified according to the Scheme, has created a Mark of Conformity with the Scheme (hereinafter, the Scheme Mark, or the Mark). The AEPD, through a contract, may grant the Certification Entities the rights to use the Mark (Annex II.B).

Certification Bodies, Training Bodies and Data Protection Delegates may make use of the Scheme Mark in the terms established in the Annex
II.A.

The Certification Entities are responsible for ensuring compliance with the trademark use regulations, both by themselves and by the training entities, which have recognized their training programs, and by the data protection delegates to the they have certified.

4 SCHEME COMMITTEE

The AEPD is responsible for the development, review and validation of the DPD Certification Scheme periodically, and at least every five years, being able to review before if the conditions of its application so advise. For this, it has created and maintains a Technical Committee of the DPD Certification Scheme (hereinafter, the Scheme Committee, or Technical Committee), as a mechanism to contact and involve the different parties interested in the certification of people for the development of the functions of the Data Protection Delegate. The involvement of the interested parties through the aforementioned Committee will be continuous in the validation and maintenance of the Scheme.

The Scheme Committee is constituted by the AEPD, as its owner, and by interested entities, organizations and associations.

Its organization and operating regime is governed by internal regulations.

5 OF THE CERTIFICATION BODIES OPERATING IN THE SCHEME

5.1 GENERAL REQUIREMENTS

In order to operate within the Scheme, CIs must:

- Pass the evaluation phase to be accredited by ENAC, in accordance with the requirements established in the UNE-EN ISO / IEC 17024: 2012 standard and in this Scheme
- Have signed and be in force the contract for the use of the Brand (Annex II.B)
- Comply with the code of ethics (Annex III)
- Operate from a headquarters in national territory, which will be the one that requests accreditation

The accreditation decisions of Certification Entities are the exclusive competence of ENAC. The AEPD can contribute technical personnel to form part of ENAC's audit teams as experts. This participation in no case implies responsibility of the AEPD in the decisions related to the accreditation of the CIs that are the exclusive competence of ENAC.

For these purposes, the AEPD will inform ENAC of any circumstance of which it is aware that may imply a breach of the accreditation requirements, or of the conditions to operate in the Scheme.

In order to provide transparency about the Certification Entities accredited by ENAC, the AEPD will publish on its website the following information that will be provided by ENAC: the full name of the accredited entity, its website, the accreditation date and the link to the annex accreditation technician issued by ENAC.

5.2 SPECIFIC REQUIREMENTS OF THE SCHEME

5.2.1 Relating to independence and impartiality

The Certification Entities and their staff may not carry out consulting, auditing, or advisory work on data protection and / or privacy, directly or indirectly, that compromise the independence and impartiality of the CBs in the assessment and certification tasks.

The Certification Entities must notify ENAC, in the manner determined by it, of any circumstance that could affect or alter compliance with the independence and impartiality requirements.

5.2.2 Training and examination requirements

Preserving the confidentiality of the questions is essential to maintain the level of demand, quality and reliability that the Scheme pursues. Therefore, the certification bodies must:

- Appoint a person in charge who will be the only one who can request the exams and who will take care that the exam questions are kept in the EC with the proper security measures ensuring that no leakage occurs. For these purposes, CIs must have documentary evidence of their confidentiality commitment.
- Establish the technical and organizational measures necessary to prevent candidates from obtaining or copying exam questions.

CBs must supervise that the professionals available to them for the DPD certification, especially the evaluators, comply with these obligations. In case of detecting any anomaly, they must proceed to cancel the relationship that binds them. CBs must ensure that these professionals whose services they can do without do not keep any type of documentation or reveal any information subject to confidentiality through their written commitment.

5.2.3 Requirements for evaluators

CBs are responsible for appointing evaluators in accordance with the requirements described in the aforementioned Annex VI.

5.2.4 Requirements related to the process of recognition of Training Entities

Part II of Annex I is collected

5.2.5 Requirements regarding the use of the Scheme Mark

The Certification Entities will establish procedures to guarantee that they themselves, the Training Entities whose training programs they have recognized and the DPOs who

has certified use the Mark of the Scheme in accordance with the rules and the contract of use, set out in Annex II.A and B, respectively. These procedures must ensure that these standards are known by the RUs and certified DPOs, that they have to contractually commit to respect them, and that proper control of their use is exercised and measures are taken in the event of a non-compliant use of the Brand. what is established in said regulations.

The AEPD may at any time request information on said procedures.

5.3 EVALUATION PROCESS

Entities interested in operating in the scheme must request accreditation from ENAC, for which they must present:

- Accreditation application established by ENAC that includes all the information stipulated therein (available at www.enac.es)
- Trademark use contract signed with the AEPD (Annex II.B)
- Responsible declaration of compliance with the code of conduct established in Annex III

Upon receipt of said documentation, ENAC will proceed in accordance with the provisions of the Accreditation Procedure and, once the application has been accepted, will inform the AEPD.

During the evaluation process, interested entities must:

- Prepare 300 examination questions that must be approved by the AEPD, as provided in clause 7.5.2.
- Carry out two exam calls, once the questions have been approved by the AEPD, with a minimum of 5 and a maximum of 15 candidates in each one who meet all the prerequisites required in the Scheme.

  The interested entity must inform the candidates who examine in the evaluation phase that it is an exam conditional on obtaining accreditation, so that those who have passed the test will obtain their certificate only when the entity has been accredited and provided that, in the audit prior to obtaining the accreditation, no irregularities have been detected that affect any of the phases of the examination process.

Likewise, interested entities may only recognize a training program, and must inform the RUs that such recognition is subject to obtaining their

accreditation as a Certification Entity. Training cannot begin until accreditation by ENAC is obtained.

Interested entities may not offer or advertise services related to the AEPD-DPD Scheme until they have ENAC accreditation.

After six months from the presentation of the accreditation application without the interested entities having obtained it for reasons attributable to them, it will automatically lapse, without prejudice to the termination of the trademark use contract (see clause 5.4 and Annex II.B).

When the AEPD becomes aware of the breach by an entity interested in obtaining ENAC accreditation of the conditions of the Scheme, including the commitments of the code of ethics, it will notify ENAC that it will act in accordance with the Accreditation Procedure. Notwithstanding the foregoing, in these cases, the AEPD, with reason and after hearing the other party, may terminate the trademark use contract.

5.4 NON-COMPLIANCE WITH THE SCHEME REQUIREMENTS

ENAC will act in accordance with the provisions of the Accreditation Procedure in the event of non-compliance with the accreditation requirements that are revealed in the follow-up audits, or in any other way and at any time.

ENAC will immediately inform the AEPD of the suspension or withdrawal of the accreditations granted, as well as the reasons that justify it, which may lead to the termination of the contract for the use of the Mark.

The resolution of the contract for the use of the Mark, without prejudice to the actions that ENAC may proceed in accordance with the Accreditation Procedure, will imply that the affected entity will not be able to offer certification services within the AEPD - DPD Scheme and, consequently, the automatic termination of accreditation.

The AEPD will not sign contracts for the use of the Mark with entities whose accreditation has been withdrawn by ENAC, or which has expired until 2 years have elapsed from the date of withdrawal or termination.

In the event of withdrawal or termination of the accreditation, the affected entities:

- They must immediately inform the DPOs that they have certified in accordance with the Scheme of this situation, so that they can go to another CB to have their certification recognized and allow them to renew it as established in the Scheme, without no additional requirements are imposed on them.

  The CBs addressed by the DPOs will assume the corresponding obligations to grant the Scheme certification.

- They must immediately report this situation to the RUs whose training programs they have recognized, so that they can turn to another CB for recognition. The RUs must request recognition following the procedure established in the CB to which they are addressed.

6 CODE OF ETHICS

In order to justify issues such as integrity and a high level of ethical commitment on the part of the entities interested in being accredited as certification entities under the AEPD-DPD Scheme, the accredited entities and the entities that offer training programs under the Scheme must observe the principles, values and commitments that are included in the Code of Ethics that is part of the Scheme as Annex III.

The Code of Ethics must be accepted by the entities interested in obtaining accreditation at the time of requesting it.

The Code of Ethics must be accepted by the entities interested in obtaining recognition for their training programs together with the request for such recognition.

CBs and RUs must give visibility to their ethical commitments by publishing the Code of Ethics on their website.

Failure to comply with the code of ethics may be cause for termination of the contract for the use of the Brand (see clause 5.4 and Annex II.B).

ENAC will immediately inform the AEPD of any circumstance of which it becomes aware that may imply a breach of the Code of Ethics.

7 CERTIFICATION PROCESS FOR DATA PROTECTION DELEGATES

The Scheme establishes the competence requirements for the person who performs the position of Data Protection Delegate, as well as the criteria to evaluate their possession by the applicants, so that, when the result of such evaluation process is favorable , the certification body will issue a statement of compliance or certificate.

7.1 PROFILE OF THE DATA PROTECTION DELEGATE POSITION

The DPD is a professional whose functions are included in article 39 of the RGPD and in articles 36 and 37 of the LOPDPGDD, and is in charge of the application of the legislation on privacy and data protection.

The DPD shall have at least the following functions:

a) inform and advise the person in charge, or the person in charge of the treatment, and the persons authorized to process the personal data under their direct authority, by virtue of the RGPD, the LOPDPGDD and other data protection provisions of the EU or its States members;
b) supervise compliance with the provisions of the RGPD, the LOPDPGDD and other data protection provisions of the EU or its Member States, and of the policies of the person in charge or the person in charge of the treatment regarding the protection of personal data;
c) supervise the assignment of responsibilities;
d) supervise the awareness and training of the personnel involved in the processing operations;
e) supervise the corresponding audits;
f) offer the advice that is requested about impact assessments related to data protection and monitor their application in accordance with article 35 of the RGPD;
g) Cooperate and act as an interlocutor with the supervisory authority for matters relating to the processing of personal data, including the prior consultation referred to in article 36 of the RGPD.

The DPD will perform its functions paying due attention to the risks associated with the processing operations, taking into account the nature, scope, context and purposes of the processing.

To do this, you must be able to:

a) collect the information necessary to determine the processing activities;
b) analyze and verify the compliance of the processing activities with the applicable regulations;
c) inform, advise and issue recommendations to the person in charge or the person in charge of the treatment;
d) collect information to supervise the registration of processing operations;
e) advise on the application of the principle of data protection by design and by default;
f) advise on:
- whether or not a data protection impact assessment should be carried out and which areas or treatments should be subject to internal or external audit,
- what methodology should be followed when conducting a data protection impact assessment,
- whether the data protection impact assessment should be carried out with own resources or through outsourcing,
- what safeguards (including technical and organizational measures) to apply to mitigate any risk to the rights and interests of those affected,
- whether or not the data protection impact assessment has been carried out correctly and
- if your conclusions (to continue with the treatment or not and what safeguards to apply) are in accordance with the RGPD;
g) prioritize its activities and focus its efforts on those issues that present the greatest risks related to data protection;
h) advise on what internal training activities to provide to staff and managers responsible for data processing activities and which processing operations to devote more time and resources;
i) intervene in the event of a claim before the data protection authorities.

7.2 COMPETENCES REQUIRED TO THE POSITION OF DATA PROTECTION DELEGATE.

The DPD must gather specialized knowledge of law and practice in the field of data protection. Consequently, the necessary knowledge, skills and abilities that the person to be certified must possess in order to carry out each of the functions of the position of Data Protection Delegate have been identified.

The generic functions of the DPO can be specified in advisory and supervisory tasks, among others, in the following areas:

1. Compliance with principles relating to treatment, such as limitation of purpose, minimization or accuracy of the data.
2. Identification of the legal bases of the treatments.
3. Compatibility assessment for purposes other than those that led to the initial collection of the data.
4. Determination of the existence of sectoral regulations that may stipulate specific treatment conditions other than those established by the general data protection regulations.
5. Design and implementation of information measures for those affected by data processing.
6. Establishment of procedures for the reception and management of requests for the exercise of rights by the interested parties.
7. Assessment of the requests for the exercise of rights by the interested parties.
8. Hiring of processors, including the content of the contracts or legal acts that regulate the responsible-person in charge relationship.
9. Identification of the instruments for international data transfers appropriate to the needs and characteristics of the organization, and the reasons that justify the transfer.
10. Design and implementation of data protection policies.
11. Data protection audit.
12. Establishment and management of records of treatment activities.
13. Risk analysis of the treatments carried out.
14. Implementation of data protection measures from the design and data protection by default appropriate to the risks and nature of the treatments.
15. Implementation of security measures appropriate to the risks and nature of the treatments.
16. Establishment of data security breach management procedures, including risk assessment for the rights and freedoms of those affected and notification procedures to supervisory authorities and those affected.
17. Determination of the need to carry out impact assessments on data protection.
18. Carrying out impact assessments on data protection.
19. Relations with supervisory authorities.

20. Implementation of training and awareness programs for staff on data protection.

7.3 PREREQUISITES

To access the evaluation phase, it will be necessary to fulfill any of the following prerequisites:

1) Justify a professional experience of at least five years in projects and / or activities and tasks related to the functions of the DPO.

2) Justify a professional experience of at least three years in projects and / or activities and tasks related to the functions of the DPO, and a minimum recognized training of 60 hours in relation to the subjects included in the Scheme program.

3) Justify a professional experience of at least two years in projects and / or activities and tasks related to the functions of the DPO, and a minimum recognized training of 100 hours in relation to the subjects included in the Scheme program.

4) Justify a minimum recognized training of 180 hours in relation to the subjects included in the Scheme program.

The conditions for the justification of the prerequisites are detailed in Annex I of this Scheme.

For these purposes, the hours of training, whether online or in person, will be counted the same, provided that the rest of the training requirements established in the Scheme are met.

All the experience acquired, both before and after the publication of the RGPD (BOE of May 4, 2016) and carried out at the national and European Union level will be valued.

The training entities shall request the certification entities to recognize the training programs they teach in accordance with the criteria and procedure established in part II of Annex I.

In case of not complying with the required experience, up to one year of experience may be validated by justifying additional merits.

7.4 CODE OF ETHICS

In order to justify issues such as integrity and the high level of professional ethics that the DPD function implies, an ethical code with principles, values and commitments has been drawn up and forms part of the Scheme, which must be accepted by the candidates. to obtain the certification prior to its granting. The code of ethics is included in Annex IV.

7.5 ASSESSMENT METHOD

The evaluation process is based both on the assessment of knowledge and experience and on continuous professional development.

Through the corresponding evaluation tests, the candidate must demonstrate that they have the appropriate competence, that is, the theoretical knowledge, the professional capacity and the personal skills necessary to carry out the functions corresponding to the activity of Data Protection Delegate. , under the terms and conditions established by the AEPD Certification Scheme.

7.5.1 Exam

The evaluation of technical or professional knowledge and skills will be carried out by taking an exam, with the following characteristics:

The exam will deal with the topics related to the specific knowledge indicated in the Scheme program, detailed in section 7.5.3, in accordance with the weighting criteria established for each of the domains in which the corresponding knowledge and competencies are structured. evaluate.

Passing the exam is an essential requirement for obtaining the certificate. The objective of the exam is to evaluate the theoretical-practical knowledge of a candidate to perform the functions of Data Protection Delegate.

The exam consists of answering 150 multiple choice multiple choice questions. 20% of the questions, that is, 30 questions, will describe a practical scenario (of a normative, organizational and / or technical nature) on which the question will focus.

The questions are distributed in each of the corresponding blocks or domains of the program according to the following weighting:

- Domain 1 - 50%, 75 questions, of which 15 with a practical scenario.

- Domain 2 - 30%, 45 questions, of which 9 with a practical scenario.
- Domain 3 - 20%, 30 questions, 6 of them with a practical scenario.

To pass the test, it is required to have answered 75% correctly (at least 113 points), as follows: 50% correct answers in each of the blocks or domains. That is, 75 points must be obtained by adding the minimum score of the three domains, and the rest of the score until obtaining 75% of the total can be obtained from any of the domains.

The questions will have four answer options, of which only one will be valid. Each correct answer will count as 1 point. Questions whose answer is incorrect or left blank are not scored.

The duration of the exam is four hours.

The result of the evaluation test will lead to the assessment of "suitable" or "not suitable" in each call.

Each certification entity will carry out the calls it deems appropriate, and must communicate its date of celebration to the AEPD at least 1 month in advance.

By agreement of all the certification bodies, unique and coordinated calls can be established.

The tasks of supervision and correction of exams can be carried out by administrative personnel of the CIs as long as they are subject to the duty of confidentiality by means of a commitment that is recorded in writing.

If no allegations are produced during the examination process by the candidates, the correction will go directly to the opinion process without the need for review by the evaluator.
If any allegation is produced in the examination process, it must be previously evaluated by the evaluator who will be the one who will rule on it, signing the corresponding report.

The correction process, as well as, where appropriate, the management of allegations by the evaluator must be anonymous for the person who corrects and for the evaluator.

The evaluator must guarantee the independence of criteria, by issuing a record with the result of the evaluation of the candidate on which the decision to grant the certificate is based.

CBs must inform the candidates of the result of the exam and for this they will use the report model that is included in Annex VII.

It is not allowed to facilitate or show the exams to the candidates who request it.

7.5.2 Question bank

The AEPD has a question bank that draws on the contributions of all entities accredited by ENAC, and, depending on the needs that the bank may present, it will require annual contributions from the CBs of questions that cover those matters not covered, or scarcely dealt with in the available questions, in the question bank, or the legislative or technological developments that are produced, prioritizing questions on deficit domains.

CBs will not be able to provide exam questions to RUs or accept questions from RUs to increase the AEPD question bank.

Interested entities, in order to be accredited by ENAC, must prepare 300 questions following the criteria established by the AEPD, in the document that will be sent to them when ENAC informs them that the entity's request has been accepted and is in the evaluation process for be credited. This document is confidential, so it will only be provided to the persons in charge of preparing the questions, who must commit in writing to keep that nature of the document.

People who have access to the document containing the requirements for writing the questions are expressly forbidden to use it for any other purpose, as well as, based on their criteria, to develop and market question models.

The AEPD will carry out two reviews of the questions and if they do not comply with the established criteria, it will inform the interested entities of the deficiencies observed. If, after the second review, the questions continue not to meet the criteria established in order to be approved, this requirement will be deemed not to have been fulfilled, and the exams will not be able to take place. If the 300 questions are validated by the AEPD, the entity in the process of evaluation to obtain accreditation by ENAC may call the exams using the aforementioned questions.

The entities that are in the evaluation process to obtain accreditation by ENAC, as well as the CBs, must notify the AEPD of the dates on which they plan to hold exams at least one month in advance. Specifically, they must provide information on the day, time and place where the exam will be held (center, street, number and city).

The AEPD will prepare the exam using the question bank and will send it, through the system established in the AEPD, to the Certification Entity for review. Once reviewed, the AEPD will send the Certification Entity an encrypted file containing two versions of the exam so that they can alternate between the candidates, as well as the correction templates and a statistics form that must be returned to the AEPD once the tests have been corrected. exams.

The AEPD may set the format in which the questions must be submitted, as well as the technical and procedural requirements to ensure the quality and confidentiality of their delivery. For this, it provides a secure system for the exchange of documents. Questions or exams may not be submitted to the AEPD by means other than this system.

The commercialization of the exam questions to which the CBs have had access in the exercise of their certifying functions, as well as elaborating model questions following the criteria of the AEPD with the same purpose, is not allowed, which includes the publication of catalogs with batteries. of questions.

The AEPD may develop a model question game that will be publicly available.

7.5.3 Program or List of Contents

The contents to be evaluated in the certification exam are integrated into the following domains or subject areas according to the indicated weightings:

Domain 1	GENERAL REGULATIONS ON DATA PROTECTION. Regulatory compliance with European regulations, national regulations, European directive on ePrivacy. Guidelines and guides of the European Data Protection Committee, etc. Weighting: 50%.
Domain 2	ACTIVE LIABILITY. Risk assessment and management of personal data processing, data protection impact assessment, data protection by design, data protection by default, etc.

Weighting: 30%.

Domain 3 TECHNIQUES TO ENSURE COMPLIANCE WITH THE REGULATIONS ON THE PROTECTION OF DATA AND OTHER KNOWLEDGE. Security audits, data protection audits, etc.

Weighting: 20%.

The contents of the agenda are specified in Annex V.

7.6 CRITERIA FOR CERTIFICATION

7.6.1 Requests and process development

Those who wish to obtain the certification as DPD must comply with the prerequisites established in section 7.3 and submit the following documentation to any of the CBs:

a) Application form
b) Detailed CV
c) Documentation justifying compliance with the prerequisites
d) Justification of the payment of the corresponding fee

Through this application, the candidate declares to know the certification process described in this document and agrees to participate in the evaluation tests.

Once the application is submitted, the CB will proceed to verify if the documentation is complete and justifies the required requirements.

If the documentation is not complete, the candidate will be informed in writing of the deficiencies noted, and a period of 10 working days will be granted to correct them. Once this period has elapsed without the correction having been carried out, the candidate will be declared as not admitted, which will also be communicated in writing.

If the application is accepted, the candidate will be informed in writing, in the same way it will proceed if the admission was for a call other than the one requested, if there are several.

Any decisions of the CB regarding the acceptance process may be the subject of the corresponding claim under the terms established in section 8 of this Scheme.

A call is understood to be the announcement of the completion of the assessment tests by a CB, on a specific date and examination center.

To access the exam, applicants must present documentation that proves their identity.

Candidates who do not pass the evaluation test will be informed, prior to taking the new test in the event that they have the right to a second test, of their result in writing, in accordance with the model contained in Annex VII.

7.6.2 Award of the certificate.

The CBs will grant the certification to the candidates who have obtained the "pass" result, and will issue them a supporting certificate, in accordance with the model that is included in the Annex VIII, which will be sent to each of them.

For the issuance of the certification, it will be a prerequisite that the candidate expressly undertakes to observe the Code of Ethics and the rules for the use of the Certificate Mark.

The CBs will assign each DPD that has certified a non-transferable personal number that will be used in the future for identification, together with the identification number of the certification body that issued the certificate.

The certificate issued will have a validity period of three years, except for sanction of suspension or withdrawal of the certification. The period of validity will start from the date of granting the certificate.

7.6.3 Maintenance

In the event that legal or technological changes occur during the period of validity of the certificate that, in the opinion of the Scheme Committee, make a significant revision or adaptation of the certificate granted convenient, the appropriate criteria may be established to maintain the validity of the certificates already granted.

7.6.4 Renewal of Certification

The renewal of the certificate will require the candidate to justify having completed:

- a minimum of 60 hours of training received and / or imparted during the validity period of the certificate, requiring a minimum of 15 hours per year in subjects covered by the Scheme program, and,

- At least one year of professional experience in projects and / or activities and tasks related to the functions of the DPO and / or information security, evidenced by a third party (employer or similar).

The training given with twice the hours of the training received will be valued.

For the training received to be considered valid, it must provide a demonstrable update of the knowledge covered by the Scheme and only the training received during the validity period of the certification will be taken into account. Recognized training to take the certification exam will not be valid.

For the training certificate to be valued, the training entity that imparts it and the title of the training, date and number of hours, agenda and format (face-to-face or online) must be stated. In the case of not being able to justify the minimum annual training required during any of the three years required, completion of this training is allowed in one of the other two remaining years. Attendance at seminars and conferences is considered training as long as the candidate provides a certificate with the same information requested for a training program.

The CB will notify the certified person of the end of the validity period of the certification at least three months in advance.

The renewal must be requested prior to the expiration date of the validity period of the certificate. The non-receipt by the certified person of the communication from the CB, informing the end of the validity period of the certification, will not exempt from compliance with what is indicated in this section.

The candidate must submit the renewal request to any of the CBs together with the list of claims that, if applicable, have been submitted during the full period of validity of the certification due to deficient actions in the activity for which they are certified. , or a statement stating that you have not been the subject of any claim. It must accompany the acceptance of the Code of Ethics and the rules for the use of the Certificate Mark, as well as the justification for payment of the renewal fees.

The Certification Entity will proceed to assess the application and the documentation provided. If as a result of the assessment it is concluded that the requirements for the renewal of the certification are not met, the interested party will be notified in writing of the deficiencies noted and a period of 90 calendar days will be granted to proceed to correct them. After this period has elapsed without its correction, the candidate will be declared as not renewed, which will be communicated in writing and the certificate will be withdrawn.

If the request is accepted, the interested party will also be informed in writing.

The renewal of the certification will imply a new supporting certificate to be issued by the CB with the same personal number assigned in the first certification. The new certificate will have a validity period of three years.

7.7 SUSPENSION OR WITHDRAWAL OF CERTIFICATION

7.7.1 Voluntary temporary suspension

In the event that the certified person declares to have ceased to comply with the requirements of the Scheme, contractual or otherwise, his certification will cease to be in force for a period not exceeding 12 months.

For the reactivation of its validity, the certification body will carry out the appropriate checks aimed at verifying that the causes that motivated the request for suspension have disappeared, provided that no more than one year has elapsed since the date of suspension of the certification and it is justified. documentary evidence that you are in a position to obtain the certificate, under the terms established for its renewal in the previous section.

Once a year of suspension of the certificate has elapsed, without it having been possible to reactivate its validity, or the causes that motivated the suspension have not disappeared, the certification will be definitively withdrawn and the interested party must, where appropriate, restart the whole process to get the same again.

7.7.2 Temporary suspension for conduct contrary to the Scheme

The following are reasons for suspension of certification by the certification body:

- The non-presentation by the certified person of the documentation, records or any information that has been required from the DPD by the certification body to maintain it, or to investigate a claim against their performance.

- Failure to perform any of the functions and tasks as DPD, as well as the lack or absence of competence for any task assigned under this Scheme.

- The realization by the person of declarations or uses in his condition of certificate that exceed the scope of the certification, that are misleading or that in any way harm or discredit the Certification Scheme.

- Behaviors contrary to the Code of Ethics.

- The use of the Scheme Mark in a way that is not permitted or contrary to the rules of its use.

- Breach by the certified person of any other of the Scheme rules that affect him.

Any of these breaches may lead to the temporary suspension of the certification for a maximum period of six months. The accumulation of three non-compliances may lead to the suspension of the certification for a period between six months and half of the cycle of validity of the certification, which in case of exceeding the term of validity will proceed to its withdrawal.

If, as a consequence of the investigation of these assumptions, the certification body concludes that there is evidence that the DPO has ceased to comply with the requirements of the Scheme, contractual or otherwise, including the possession of a certain competence, and consequently your certificate is no longer valid, the CB shall proceed to temporarily suspend said certificate until the causes that motivate it are remedied.

The sanctions established will be understood without prejudice to the civil, criminal, professional or other responsibilities that certified DPDs may incur in the exercise of their profession.

For the reactivation of the certificate, the CB will carry out the appropriate checks to verify that the causes that motivated the suspension have disappeared, and a partial or total re-evaluation may even be required.

7.7.3 Withdrawal of certification

The following are reasons for the withdrawal of a certification already issued:

- Any of those identified above for the temporary suspension, depending on its severity or its repetition, such as reiteration in a specific type of

non-compliance that would have resulted in a temporary suspension, which implies that the DPD's conduct has not been corrected.

- The accumulation of more than three sanctions for suspension of certification.
- The lack of collaboration of the certified person for the return of the certificate in case of sanction.

Stakeholders whose certification has been withdrawn by the CBs and who wish to obtain it again must undergo a complete initial certification process. The CBs may require these people so that, prior to undergoing the evaluation, they demonstrate that they have corrected the causes that led to the withdrawal of the previous certificate without this being considered discriminatory treatment.

The CBs will reserve the right to accept a new request by the sanctioned professional.

7.8 RIGHTS AND OBLIGATIONS OF CERTIFIED PERSONS

7.8.1 Rights

Certificate holders will have the right to:

- Make use of the certificates for the development of your professional activity.
- Benefit from all the dissemination and promotion activities carried out by the certification body regarding certified persons.
- Make use of the Mark of the Scheme in accordance with the provisions of Annex II.
- Claim and appeal any unfavorable decision.

7.8.2 Obligations

The holders of the certificates will be obliged to:

- Respect the DPD Certification Scheme and all applicable procedures.
- Comply with the financial obligations derived from the certification.
- Accept the prescriptions of the Code of Ethics.
- Act in their professional field with due technical competence, ensuring the maintenance of the prestige of the certification granted.
- Collaborate with the certification body in the activities of supervision of its performance necessary for the maintenance and renewal of the certification.

- Inform the certification body about any professional situation that could affect the scope of the certification granted.
- Inform the certification body, without delay, about issues that may affect it to continue meeting the certification requirements.
- Not to use the Scheme certificate for purposes other than those derived from carrying out activities within the scope of the certification granted.
- Not to carry out harmful actions of any nature, nor to damage the image and / or interests of people, companies, entities and clients, even potential ones, interested in the professional service, nor that of the AEPD or the certification entities.
- Not to take part in fraudulent practices related to the theft and / or disclosure of examination material.
- Maintain a record of complaints received in relation to the scope of the certification obtained.
- Return the certificate in case of withdrawal of the certification.

Failure to comply with the obligations described will start the process of suspension or withdrawal of the certificate.

7.8.3 Information on certified persons

The CBs will keep an up-to-date record of certified persons that will include: name and surname, certificate number, grant date, expiration date and certificate status (granted, suspended, withdrawn, renewed).

The CBs will publish the information contained in said registry on their website, and will communicate it to the AEPD by the mechanism that it designates. Likewise, the AEPD will publish said information and that of the entity that has issued the certification on its website.

The CBs are responsible for keeping this information up to date.

8 MANAGEMENT OF COMPLAINTS AND CLAIMS ABOUT THE SCHEME

8.1 SCOPE OF APPLICATION

Any actions contrary to the Scheme, including the Code of Ethics, carried out by certification entities, training entities and by certified Data Protection Delegates may be the subject of a complaint or claim.

The behaviors of certified Data Protection Delegates that are contrary to the Code of Ethics that are attached as Annex IV, as well as the behaviors of the aforementioned entities that are contrary to the Code of Ethics that are attached as Annex III, will be the object of special attention.

8.2 COMPETENT BODIES

They are competent bodies to know and, where appropriate, resolve the complaints or claims that are presented about the Scheme, and in this order:

or The Certification Entities (EC)
or The National Accreditation Entity (ENAC)
or The Spanish Data Protection Agency (AEPD)

Any complaint or claim regarding the performance of one of the Scheme Agents must be presented, first, to the Agent that made it.

a) If the claim or complaint is related to a training program recognized by a CB, it must be managed by it in accordance with the requirements of the UNE-EN ISO / IEC 17024 standard.

b) If the claim or complaint is related to the actions of the CB, it must be managed by it in accordance with the requirements of the UNE-EN ISO / IEC 17024 standard.

c) If the claim or complaint presented by a third party, either before the AEPD, ENAC or a CB, refers to the action or performance of a DPD certified in the Scheme, it must be forwarded to the rest of the agents and processed in the first instance by the CB that has certified the DPD. The responsibilities will depend on the content of said claim.

d) If the claim or complaint is related to the accreditation granted, it must be processed by ENAC, which, in addition, must process those that come from claimants dissatisfied with the response given, in the first instance, by an accredited CB.

e) If the claim or complaint refers to the breach of the Code of Ethics (Annex III) by a RU or a CB, it must be presented to the complained entity, which must communicate it, together with the response provided, to the CB, in the event that has been directed against an EF and, in any case, the AEPD.

The treatment given to claims and complaints, as well as their resolution, will be verified by ENAC as part of its evaluation.

The AEPD may only intervene in the management and treatment of any claim or complaint received in relation to the operation of the Scheme if, previously, it has been processed by the other Scheme Agents.

Any claim addressed to the AEPD about the Scheme must be formally communicated in writing, identifying that it is a claim or complaint, and that a resolution has previously been attempted before the corresponding Scheme Agent (EC or ENAC, or both).). The AEPD will adopt the corresponding resolution that will notify the claimant.

8.3 COMPLAINTS AND CLAIMS PROCEDURE.

The process for the treatment and resolution of complaints or claims will be established by the corresponding EC in accordance with the UNE-EN ISO / IEC 17024 standard, which must be available to the public.

The procedure for managing complaints or claims about the Scheme must follow, at least, the following procedures:

a) Study and assessment of the complaint or appeal and, where appropriate, request for evidence.
b) Communication to the interested parties and / or affected by each appeal and claim process regarding the situation revealed, including a maximum period of 30 days for the presentation of allegations.
c) Analysis and evaluation of the evidence provided and the allegations presented by the interested parties.
d) Deliberation and final decision-making in this regard.
e) Communication of the resolution to the parties.

For the proper development of this procedure, the certified person is obliged to:

a) Cooperate fully with any formal investigation open to resolve specific cases of claims and / or complaints.
b) Maintain a record of all claims filed against it for the activity carried out within the scope of validity of the certification, and allow the CB access to these records. For this purpose, within ten days from the receipt of the claim, it must be communicated in writing, together with a copy of the claim, to the EC.
c) Provide clients with a form to formalize any complaint related to the services provided, which will be sent both to the certified person and entity affected by the complaint, as well as to the Certification Entity.

If the complaint or claim gives rise to the opening of an investigation activity on a certified person, whose resolution could imply the temporary suspension or the withdrawal or loss of the certification obtained, the provisions of section 7.7 of this Scheme will be followed.

9 MONITORING AND SUPERVISION OF THE SCHEME

In order to guarantee the necessary quality and rigor standards in compliance with the Scheme by the corresponding Agents, a Monitoring Committee is constituted made up of members of the Spanish Agency for Data Protection and the National Accreditation Entity to monitor and control of its operation.

Additionally, ENAC and the AEPD will share information regarding the operation of the Scheme in their respective areas of action to ensure that the Scheme works in a coherent manner and is consistent with the highest levels of demand.

10 TRANSITIONAL PROVISION

This Scheme will be applicable to entities interested in obtaining accreditation, certification entities, training entities and data protection delegates from the day after its publication on the AEPD website, remaining the provisional designations that have been issued have since expired.

For interested entities that, upon publication of this version, had already accepted the documentation in ENAC or had been issued the provisional designation, the term for accreditation remains 12 months from the date the request was formalized, and they must not However, comply with the requirements of this Scheme to be accredited,

which will be verified through the procedure established therein. For these purposes, within a period of 1 month from the publication of this Scheme, the contract for the use of the Scheme Mark must be signed and sent to ENAC in accordance with the model in Annex II.B. and the responsible statement in which it declares to comply with the ethical code established in the Annex III. Failure to sign the contract or the responsible declaration will determine the impossibility of continuing with the accreditation procedure.

The accredited entities, within a period of 1 month from the publication of this Scheme, must sign a new contract for the use of the Mark adapted to the model in Annex II.B. and the responsible statement in which it declares to comply with the ethical code established in the Annex III. Failure to sign the contract or the responsible declaration will determine the termination of the contract in force and the termination of the status of Scheme Agent.

Likewise, accredited entities have a period of 3 months from the publication of this Scheme to replace the certificates issued to certified DPOs with new ones that incorporate the updated logo. In addition, they must inform the EFs with recognized programs that within that period they have to change the logo on their web pages and update theirs.

The CBs have a period of 1 month, from the publication of this Scheme, to require the RUs that have recognized their programs to sign the responsible declaration in which they declare that they comply with the Code of Ethics. Failure to sign the declaration of responsibility will determine the withdrawal of recognition of the training programs.

Accredited entities and training entities must, within 3 months from the publication of this Scheme, submit a responsible declaration in which they declare that they comply with the requirements relating to independence and impartiality contained in it.

ANNEXES

Annex I. Conditions for the justification of the prerequisites and the process of recognition of training programs Annex

II. Scheme Brand

or Annex II.A. Rules for use of the Scheme Mark
or Annex II.B. Model contract for the use of the Scheme Mark

Annex III. EC and EF Code of Ethics

Annex IV. Code of Ethics DPD

Annex V. Program (agenda) of the Scheme

Annex VI. Selection procedure and appointment of evaluators

Annex VII. Model of report of the results of the examination Annex

VIII. Model document justifying the certification

ANNEX I

CONDITIONS FOR THE JUSTIFICATION OF THE PREREQUISITES AND THE PROCESS OF RECOGNITION OF THE TRAINING PROGRAMS

I.- CONDITIONS FOR THE JUSTIFICATION OF THE PREREQUISITES.

Candidates to attend the certification processes as DPD must prove the training and professional experience requirements in the following terms:

A. TRAINING.

Provide a certificate of having received the necessary and recognized training in relation to the subjects covered by the Scheme program in order to be able to sit the exam, stating:

- Training entity that issues the certificate.
- Certification body that has recognized the program.
- The training received (60, 100 or 180 hours).
- The distribution of the training hours of the program according to the percentage established for each of the domains of the Scheme program. A program of Training can be made up of several courses.

  or For the 60-hour training, the distribution will be as follows:

  Domain 1 - 30 hours, Domain 2 - 18 hours, Domain 3 - 12 hours

  or For the 100-hour training, the distribution will be as follows:

  Domain 1 - 50 hours, Domain 2 - 30 hours, Domain 3 - 20 hours

  or For the 180-hour training, the distribution will be as follows:

  Domain 1 - 90 hours, Domain 2 - 54 hours, Domain 3 - 36 hours

For training expressed in ECTS credits[1] or LRU[2] (referring to university training, including internships or the end of the degree project), it is considered that 1 ECTS is equivalent to 25 hours and 1 LRU to 10 hours.

In the computation of hours for the justification of the training acquired with respect to domains 2 and 3, both the one obtained before and after the publication of the RGPD (BOE of May 4, 2016) will be valued. Therefore, the candidate does not need to take a complete training program of 60, 100 or 180, but only that subject that he needs to complete the required training hours following the criteria of the Scheme.

B. WORK OR PROFESSIONAL EXPERIENCE.

Justify work or professional experience of two, three, or five years in projects and / or activities and tasks related to the functions of the DPO (obtained before or after the publication of the RGPD). For this, the candidate must provide:

a) Employee who has performed his functions within a company as an employee: certificate of working life and certificate of the company stating the tasks performed in relation to data protection, start date and end date .

b) Self-employed worker who provides his services to different clients: certificate of working life and certificate of clients stating the tasks performed in relation to data protection, start and end date of the services provided, adding in total the required years of experience.

c) Worker in a consulting company, that is, the employee of a consulting firm that provides services to different companies: certificate of working life and certificate of the consulting firm stating the tasks performed in relation to data protection, date of start and end of the work carried out.

d) Independent worker who provides his services to consulting companies: certificate of working life and certificate of the consulting firm.

Years of experience (2, 3, or 5) are full time. Dedication is calculated based on the 225-day annual working day, and that a working day is considered full if it justifies 8 hours of dedication.

[1] Credits according to the European Credit Transfer System.

[2] Credits according to the University Reform Law of 1983.

Experience in the processing of high-risk personal data with twice the time than the years of experience in the processing of personal data that does not involve that level of risk will be especially valued.

In the event that the experience is not for a full year, the experience that equals or exceeds six months will be assessed with half of the annual score.

Only if the required experience is not achieved, up to one year of experience can be validated through validation of additional merits, that is, up to 60 points.

As work experience, the training given will also be considered and, specifically, it will be valued with twice the hours of the training received.

The training given in a specific subject will only be considered accepted one of the editions given, if there is more than one with the same title and agenda.

For the evaluation of the experience, the scale in table 1 will be applied.

Table 1

Training	Experience	Year Score experience	Minimum score of years of experience
-	5 years	60 points	300 points
60 hours	3 years	60 points	180 points
100 hours	2 years	60 points	120 points
180 hours	-		

C. VALIDATION OF ADDITIONAL MERITS

If the score required by the professional experience prerequisites is achieved, it will not be necessary to assess any additional merit. Only in the case that the minimum score required is not exceeded due to lack of years of experience, the following table of merits will be used to supplement punctuation.

Aspects already considered as prerequisites will not be evaluated as merits.

For the assessment of additional merits, the scale in table 2 will be applied.

Table 2

Category	Punctuation Maximum	Merit	Points unitary[3]	Max.
Training university specific or complementary in Data Protection or privacy, depending on EHEA.[4]	30	Degree, diploma or technical engineering	6	12
		Postgraduate or Master's own degree Official	6	12
		postgraduate	8	16
		Official Master	10	twenty
		Doctorate	9	9
Training specific or complementary, in Data Protection or privacy.	fifty	Attendance at courses, seminars, events, acts or congresses organized or expressly recognized by Data Protection Certification Authorities or Entities (minimum 1 credit or 10 h.)	1	25
		Attendance at non-university courses or seminars organized by professional organizations (minimum 2 credits or 20 h.)	0.20	10

[3] Attributable to each merit individually considered. In specific cases such as attendance at events, it will be considered that a unit is reached when the total minimum recognized hours is credited.
[4] According to the EHEA: European Higher Education Area.

Category	Punctuation Maximum	Merit	Points unitary[3]	Max.
		Attendance to courses or seminars university students (minimum 2 credits or 20 h.)	0.50	10
		Attendance at events, acts or congresses of the specialty that must total at least 20 h. year.	0.50	5
End of course work on Data Protection or privacy.	5	Completion of end-of-course work with a dedication of at least 40 hours.	1	5
Internships in companies on topics protection of data or privacy.	5	Carrying out an internship in companies with a dedication of at least 40 hours.	1	5
Teaching activity related to area of Data Protection or privacy.	30	Teaching in university degrees (for every 10 h.)	0.5	10
		Teacher in level courses / seminars basic (for every 20 h.) Teacher courses andseminars from specialization (for every 10 h.)	0.2	5
		Teacher in Certification Entities from courses (for every 10 h.)	0.5	10
		Lecturer, speaker or communicator in congresses (per event)	0.1	5
Exercise researcher and publications in protection issues data or Privacy.	twenty	Authorship or co-authorship of books	2.5	8
		Authorship or co-authorship of book chapters, official conference proceedings and equivalents.	0.5	5
		Authorship or co-authorship of articles in specialized journals and publications.	0.25	5
		Authorship or co-authorship of contributions in the media and blogs.	0.10	2

Category	Punctuation $M_{maximum}$	Merit	Points unitary[3]	Max.
Awards Data Protection or privacy.	10	Professional awards and recognitions or similar.	5	10
Certifications in matters of Data Protection or privacy (in vigor).	10	ACP-DPO of APEP, CDPP of ISMS FORUM[5], ECPC-B DPO of Maastricht University, DPO of EIPA (European Institute of Public Administration) or similar.	5	10
Other certifications in subjects related (in vigor).	10	ACP-B / ACP-CL / ACP-CT / ACP-AL / ACP-AT de APEP, CDPP from ISMS FORUM[6], CISA / CISM / CRISC of ISACA, CISSP of Certified Information Systems Security Professional (ISC)[2], CIPP / CIPT of IAPP (International Association of Privacy Professionals), ISO 27001 Auditor or similar.	2	10

II.- PROCESS OF RECOGNITION OF THE TRAINING PROGRAMS.

The Training Entities must request the Certification Entities to recognize their training programs following the requirements established in this Annex. If necessary, the recognition requirements required by the AEPD will be published, both for the training programs and the entities that provide it, in relation to content, minimum duration of training, validation method, requirements related to training personnel. , to the means or facilities, use, etc.

CBs will recognize FE training programs in accordance with the following requirements:

- Duration (60, 100 or 180 hours).
- Subject taught in accordance with the program defined in the Scheme.

5 New CDPP since December 2016.
6 CDPP prior to December 2016.

- Validation method by passing an exam (it is not enough to justify attendance at the training).
- Didactic methodology that includes imparting theoretical knowledge, carrying out practical exercises and developing collaborative exercises with a result and expository value (group work that includes presentations and debates, either in person and / or in person).

For these purposes, the people who provide the training must have the knowledge and professional experience equivalent to or greater than that required of the candidate to be certified and with the ability to assess the training of the students. They will not be able to make the training compatible with the preparation of questions or with the role of evaluator in the certification bodies.

The distribution of the hours of the training programs should be adjusted to the following criteria:

- For the 60 hour training:
  - or Domain 1 - 30 hours.
  - or Domain 2 - 18 hours.
  - or Domain 3 - 12 hours
- For the 100 hour training:
  - or Domain 1 - 50 hours.
  - or Domain 2 - 30 hours.
  - or Domain 3 - 20 hours.
- For the 180 hour training:
  - or Domain 1 - 90 hours.
  - or Domain 2 - 54 hours.
  - or Domain 3 - 36 hours.

For training expressed in ECTS credits[7] or LRU[8] (referring to university training, including internships or the end of the degree project), it is considered that 1 ECTS is equivalent to 25 hours and 1 LRU to 10 hours.

The training programs recognized by the CBs are valid from the date of recognition and those training that start from that date will be valid. Editions prior to the recognition date are not considered valid.

RUs whose training program has been recognized by entities that are in the process of granting accreditation will not be able to start training until they have been accredited by ENAC.

The recognition of a training program by a CB will be valid for the remaining CBs in order to accredit the training as a prerequisite for access to the exam in any other CB.

Therefore, the Training Entity, once its training programs have been recognized by a CB, will not need the recognition of other Certification Entities.

The CBs will issue a training recognition certificate to the RU stating:

- Name of the Certification Entity.
- Name of the Training Entity with identification of its website.
- Name of the recognized program.
- Date of recognition.
- Duration (60, 100 or 180 hours) and criteria for passing it.
- Subject taught and distribution of hours for each of the three domains of the syllabus.
- Program format (online or face-to-face).

The certificate of recognition will include the following clause:

> «The recognition will remain valid as long as the verified requirements for obtaining it are not modified in accordance with the AEPD-DPD Scheme in its current version (program, distribution by domain, teaching methodology and method of validation), or the scheme itself in what could affect it. "

[7] Credits according to the European Credit Transfer System.
[8] Credits according to the University Reform Law of 1983.

The recognition of training programs should not compromise independence and impartiality, nor reduce the requirements for evaluation and certification, which is why CBs cannot offer training under the Scheme, using the same trademark or logo, nor trademarks or logos that may be misleading as they constitute a threat to the necessary impartiality.

CBs will publish on their website the following information on recognized training programs and those that have lost their validity:

- Name of the Training Entity with identification of its web page (the web address must point directly to the area of the web page where the training is offered).

- Name of the recognized program.
- Date of recognition.
- Duration (60, 100 or 180 hours) and criteria for passing it.
- Subject taught and distribution of hours for each of the three domains of the syllabus.
- Program format (online or face-to-face).
- Where appropriate, date and reasons for the loss of validity of the recognition.

RUs must publish clear and transparent information on recognized training programs on their website, including the following information:

- Full name of the Training Entity Name of the
- CB that has recognized the program Name of
- the recognized program
- Date of recognition of the program Duration
- and criteria for passing the program
- Subject taught and distribution of hours for each of the three domains of the syllabus
- Program format (online or face-to-face)
- List of teachers who teach each of the headings by domain Updated
- curriculum of teachers

The RU will issue the students of their training programs, a certificate stating:

- Name of the Training Entity
- Recognized program name
- Name of the CB that has recognized the program and date of recognition
- Date of completion of the program
- Duration and criteria for passing the program

- Subject taught and distribution of hours for each of the three domains of the syllabus.
- Program format (online or face-to-face)

The AEPD will publish the recognized training programs on its website, for which the CBs will send said information by the method designated by it. The CBs are responsible for keeping the list of said programs up to date.

The CBs will ensure that the training processes are developed in accordance with the recognized training activity, that they are publicized with transparency and that, in no case, there is an inappropriate use of the Brand and the logos of the entities that participate in the scheme. Periodically, and at least annually, they must carry out control activities of the recognized training programs aimed at achieving a genuine qualification of the candidates and prevent them from focusing on a simple training to pass the exam rather than on their training. Likewise, they must inform the RUs that both ENAC and the technical staff of the AEPD may attend the courses they teach in an unannounced manner in order to evaluate the effectiveness of the control systems established by the CIs.

So that RUs can improve and assess the training given, the CBs that have recognized their programs can send them statistical information on the number of approved in each call, with distribution of the results by domains or headings. This information is confidential, the CBs can only provide it to the RUs whose programs they have recognized and must ensure that the RUs do not exchange this type of information. RUs cannot publish this information on their website or use it for commercial purposes.

The AEPD reserves the right to request the RUs at any time to deliver their training programs for verification and, if they do not comply with the Scheme, they may revoke them for reasons. Likewise, they will be able to take the pertinent tests to verify the rigor of the training given and the tests carried out on their students to pass the training.

As a guarantee of independence and impartiality, CIs cannot market the training syllabus included in Annex V of the Scheme with EFs, nor can teachers who teach any subject in training programs recognized under the AEPD-DPD Scheme may be evaluators of the Scheme of certification.

Failure to comply with the requirements established for the recognition of RU training programs and their control by CIs may be grounds for termination of the trademark use contract (clause 5.4 and Annex II.B).

Spanish universities, public or private, may request the AEPD to recognize their postgraduate programs (Master's), both those that are certified by the National Agency for Quality Assessment and Accreditation (ANECA) and their own Master's degrees. Recognition will be carried out as long as the Master meets the requirements established in the Scheme.

In the recognition application, the University must indicate which Scheme program it wishes to be recognized (180, 100 or 60 hours) and, depending on it, adjust the Master's program to the domains according to the detailed distribution according to the defined domains in the Scheme. The University must attach, along with its application, a supporting report indicating in detail the correspondence of the contents of the Master in relation to the Scheme program that it wishes to recognize.

ANNEX II.A

RULES OF USE OF THE MARK OF THE SCHEME

1. THE MARK OF THE SCHEME.

In order for the market to be able to identify the certification of people as "Data Protection Delegate" (DPD) promoted by the AEPD, the AEPD-DPD Scheme Mark is created.

The Scheme Mark is the symbol used by Certification Bodies, Training Bodies and persons certified as Data Protection Delegates to make this fact public and identify them as agents of the Scheme.

It may not be used by entities or persons other than those described in the previous paragraph, nor by any entity interested in being accredited as a certification entity while it is in the evaluation process.

The design of the Scheme Mark is shown at the end of this Annex.

2. RULES OF USE.

The AEPD will grant a license for the use of the Mark, through a contract with the Certification Entities, subject to the following rules:

a) It will always be used clearly associated with the name or logo of the authorized agent.

b) CBs and RUs may use it exclusively in documents or advertising-type supports of the service they provide within the framework of the Scheme (brochures, web pages, etc.), in such a way that it is clear that they are only linked to the service provided within the Scheme. and not with any other similar service that is offered to the market.

c) Certified DPOs may use it exclusively in documents or advertising-type supports of the service they provide as DPD (business cards, brochures, web pages, etc.) and not in any other similar service whose provision they can offer to the market.

d) The Certification Entities will stop using the Scheme Mark when the user license contract ends or is terminated, as well as in the event of suspension or withdrawal of accreditation to CBs by ENAC. In these cases, the persons certified by said entities may continue to use the Mark, until the renewal of the certification, in which case, they will use that of the CB that renews it.

e) The Training Entities will stop using the use of the Trademark when the validity of the recognition of their training programs has ended, or it has been revoked. In the event that CIs must stop using the trademark, RUs may continue to use it in those training programs that are in progress at that time, otherwise they must obtain recognition of their programs from another CI to make use of the Mark.

CBs are responsible for ensuring that both they and the RU whose training programs they have recognized, and the DPOs they have certified use the Mark following these standards. In case of detecting a misuse of the Mark, they must adopt the appropriate measures, including the revocation of the recognition of the training programs and the suspension or withdrawal of the certification.

The infringement of the obligations of the CIs regarding the surveillance and control of the use of the Trademark by the EFs and the DPOs may lead to the termination of the contract for the use of the Mark.

THE CENTRAL BOX WILL INCLUDE:

- FOR CERTIFICATION BODIES, THE DATE ON WHICH THE ACCREDITATION WAS OBTAINED
- FOR TRAINING ENTITIES, THE DATE ON WHICH THE RECOGNITION OF THE TRAINING WAS OBTAINED
- FOR DATA PROTECTION DELEGATES, THE DATE ON WHICH THE CERTIFICATION WAS OBTAINED

ANNEX II.B

MODEL OF CONTRACT FOR THE USE OF THE BRAND OF THE SCHEME BETWEEN AEPD AND THE AGENTS OF THE SCHEME

In Madrid, on of 20..

TOGETHER

From one side,

From elsewhere,

Mutually recognizing the legal capacity necessary for the granting of this contract,

EXPOSE

I. That, in order for the market to be able to identify the certification of people as "Data Protection Delegate" (DPD) promoted by the AEPD, the AEPD-DPD Scheme Mark has been created, registered in .... for classes..... of the International Gazetteer.

II. That the Scheme Mark is the symbol used by Scheme Agents and certified persons to make this fact public.

III. That the mark of the Scheme is the property of the AEPD and can only be used under the responsibility of the undersigned Certification Entity under the conditions established in the Rules of Use published by the AEPD as part of the Delegate Certification Scheme of the Spanish Agency. Data Protection (AEPD-DPD Scheme).

IV. That the undersigned Certification Entity is interested in operating in the AEPD-DPD Scheme.

V. That the signing of the trademark use contract is a condition to operate within the Scheme, and it must be signed prior to applying for accreditation to ENAC, to whom a copy of this contract must be provided.

SAW. That both parties have agreed to sign this Trademark Use Agreement subject to the following:

CLAUSES

FIRST. Object

The AEPD assigns to the Certification Entity the rights to use the Scheme brand under the conditions established in the Standards for the use of the brand contained in Annex II.A and in clause 5.4 of the AEPD-DPD Scheme.

SECOND. Suspensive condition.

The use of the mark of the Scheme is conditioned on the granting of accreditation by ENAC in accordance with the Accreditation Procedure.

The Certification Entity must notify the AEPD of obtaining the accreditation in order for the AEPD to formally provide it with the corresponding trademark file, at which point its use can begin.

THIRD. Responsibility of the Certification Entity.

The Certification Body is responsible for:

a) Exercise adequate control of the use of the brand in accordance with the conditions established in the Regulations for the use of the brand contained in Annex II.A and in clause 5.4 of the AEPD-DPD scheme, both by itself and by the Entities of Training that it recognizes and the DPOs that it certifies, assuming the consequences established in the Scheme in case of breach of said obligation.

b) Inform the recognized Training Entities of the rules of use that apply to them and of their obligation to cease using the mark of the scheme in case of

termination of this contract and that said obligation is established in a contractual manner with the RUs. Additionally, the CB undertakes to take legal measures against the FIs in the event that they breach said obligation.

c) Inform certified DPOs about the applicable Rules of Use, as well as the consequences of improper use

QUARTER. TERMINATION OF THE CONTRACT.

1. The following are causes for termination of this contract:

a) The mutual agreement of the parties.

b) The expiration of the six-month period from the request for accreditation to ENAC without having obtained it, for reasons attributable to the Certification Entity.

c) Withdrawal of accreditation.

2. Likewise, it may give rise to the termination of the contract, motivated and after hearing the Certification Entity:

a) Suspension of accreditation.

b) Failure to comply with the code of ethics.

c) Non-compliance by the Certification Entity of its duty to control the use of the Mark with respect to the Training Entities that it has recognized and the DPDs that it has certified.

d) Any other breach of the obligations established in this contract.

e) Any other cause different from the previous ones foreseen in the current legislation that is applicable.

3. The termination of the contract implies that the entity cannot offer the certification services within the Scheme, giving rise to the termination of the status of Agent of the Scheme and the compensation of the damages caused.

4. Once the contract is terminated, the AEPD will not sign a new contract for the use of the brand with said entity until after two years, counting from the resolution.

FIFTH. Competent jurisdiction.

The controversies that may arise between the parties as a result of the interpretation or execution of this contract will be known and competence of the jurisdictional order. contentious-administrative.

ANNEX III

CODE OF ETHICS FOR ENTITIES REQUESTING ACCREDITATION AS CERTIFICATION ENTITIES OF DATA PROTECTION DELEGATES ACCORDING TO THE SCHEME OF THE SPANISH PROTECTION AGENCY AND THE ENTITIES THAT OFFER TRAINING

PREAMBLE

This Code constitutes an express declaration of the values and principles that, based on the applicable regulations and the requirements of the Certification Scheme for Data Protection Delegates of the Spanish Data Protection Agency (AEPD-DPD), must preside over and guide the behavior of those entities and companies (hereinafter, interested entities) that request from the National Accreditation Entity (ENAC) the accreditation to be certifying entities (hereinafter, EC) of Data Protection Delegates, in accordance with the AEPD- Scheme. DPD, in the exercise and performance of their professional activity.

The ethical code includes a set of principles and values (legality, integrity, good repute, fair competition, professionalism, responsibility, impartiality, transparency and confidentiality) that come from the obligations established by the different regulations that are applicable to the activity of the entities. that request the accreditation of EC to ENAC, as well as those included in the AEPD-DPD Scheme.

Its observance is based on due diligence for its compliance with the purpose of providing confidence and guarantee of an absolutely responsible behavior with the current legislation in its relations with employees, suppliers, clients and any third parties with whom they interact, both in the public sphere. as private, including society in general.

The objective of this code is to ensure a professional behavior on the part of the interested entities: of their managers, employees, attorneys, representatives and collaborators, that moves away from conducts and acts contrary to the principles and values that it includes.

The code of ethics, which interested entities are obliged to sign prior to submitting the accreditation application, implies the commitment to act in accordance with their

principles and values during the accreditation procedure as CB by ENAC and during the exercise of its activity as CB once they have been recognized as such.

In order for the code to be effective and to provide confidence and security to those who are related or have to be related to the entities interested in ethical behavior, they must proceed to its dissemination among managers, employees, attorneys, representatives and collaborators; establish procedures and structures for the communication and management of complaints; and for the supervision and control of its observance, functions that, where appropriate, may also be carried out by the AEPD to guarantee the proper functioning of the AEPD-DPD Scheme.

The code of ethics also applies to training entities, whose behavior within the framework of the AEPD-DPD Scheme must observe the principles and values it contains.

ARTICLE I. SCOPE OF APPLICATION

The principles and values contained in this ethical code are of mandatory observance and compliance for the entities that request from the National Accreditation Company (ENAC) to be accredited to certify DPD according to the AEPD-DPD Scheme, as well as by their managers, employees , attorneys-in-fact, representatives and collaborators, from the moment the application is submitted and during the exercise of their activity as CB within the framework of the AEPD-DPD Scheme.

It will be applicable to all companies that are part of the interested entities, including their managers, employees, attorneys, representatives and collaborators.

The code of ethics will apply to training entities, their managers, employees, attorneys, representatives and collaborators.

ARTICLE II. PRINCIPLES OF ACTION

The interested entities and their companies, their managers, employees, proxies, representatives and proxies in the exercise of their activities will behave subject to the following principles:

Legality, The interested entities will strictly comply with the legislation and regulations in force at all times, and especially with the provisions of the

AEPD-DPD scheme, in order to prevent any illegal activity from being carried out and, in particular, practices or statements that in any way harm the ENAC, AEPD, the AEPD-DPD Scheme, or any of its actors.

Interested entities undertake to adopt the necessary measures so that their managers, employees, attorneys, representatives and collaborators are aware of the applicable regulations, including the principles and values of the ethical code and can observe them.

Integrity, The interested entities will carry out their activities at all times with professional ethics, honestly, professionally and in good faith, avoiding conflicts of interest.

Honorability, The interested entities must not have been subject to sanction in any of the areas of their activity and professional practice during the three (3) years prior to the presentation of the accreditation application, nor be sanctioned during their performance as CB.

Fair competition, The interested entities will carry out their professional activity in a fair manner, without allowing deceptive, fraudulent, or malicious behavior.

In data protection they will avoid aggressive practices such as:

Act with the intention of supplanting the identity of the Spanish Data Protection Agency or an autonomous data protection authority in making any communication to those responsible and in charge of the treatments or to the interested parties.

Generate the appearance that it is acting on behalf, on behalf of or in collaboration with the Spanish Agency for Data Protection or an autonomous data protection authority in the realization of any communication to those responsible and in charge of the treatments in which the sender offer your products or services.

Carry out commercial practices in which the decision-making power of the recipients is restricted by referring to the possible imposition of sanctions for breach of the personal data protection regulations.

Offer any type of document by which it is intended to create an appearance of compliance with the data protection provisions in a complementary way to the performance of training actions without having carried out the necessary actions to verify that said compliance is effectively produced.

Assume, without express designation of the person in charge or the person in charge of the treatment, the function of data protection delegate and communicate in such condition with the Spanish Agency for Data Protection or the regional data protection authorities.

Responsibility, In the development of their professional activities, the interested entities will assume the collaboration activities required by the AEPD and other public authorities, as well as the rest of the entities of the AEPDDPD Scheme for their proper development and maintenance, avoiding any conduct that damages their reputation. .

Impartiality, Interested entities will act objectively in their relationships with third parties, without accepting pressure or influences from third parties that could question their professional integrity, or that of their managers, employees, attorneys, representatives and collaborators, in particular with the training entities of the AEPD Scheme -DPD.

Transparency, The interested entities will act with transparency in the exercise of their professional activity, specifically within the scope of the AEPD-DPD Scheme that requires:

Inform all interested parties in a clear, precise and sufficient manner of all the aspects that come together in the professional practice as a CI, as long as they are not subject to the confidentiality regime, in which case they will be reserved and cannot be disclosed. .

Provide all interested parties with clarity, precision and sufficiency all relevant information on the certification process and on the status of accreditation

Confidentiality, The interested entities will respect and keep the necessary protection and reservation of the information to which they may have access due to their activity as CB, safeguarding the legitimate rights of all parties.

interested. Such information will not be used for your benefit or that of your staff, nor will it be disclosed to inappropriate parties.

ARTICLE III. RELATIONS WITH THE ORGANIZATION STAFF

In their relationships with their employees, managers and collaborators, the interested entities:

They will provide the necessary means to communicate and disseminate the ethical code among all their employees.

They will avoid situations that may give rise to conflicts of interest with the activities of the organization.

They will establish procedures that allow the notification of conduct contrary to the ethical code and the AEPD-DPD scheme.

They will ensure that the personnel in their charge do not carry out illegal activities or conduct contrary to the ethical code and the AEPD-DPD Scheme.

They will assume responsibility for the actions of their managers, proxy employees, representatives and collaborators.

ARTICLE IV. RELATIONSHIPS WITH EXTERNAL COLLABORATORS, SUPPLIERS AND CUSTOMERS

Interested entities:

They will establish relationships based on respect for current legislation, the AEPD-DPD Scheme, ethical behavior, loyalty, good faith, trust, respect and transparency.

They will act impartially and objectively in the collaborator selection processes, applying duly documented criteria of competence and quality, avoiding at all times the collision of interests, in particular with training entities.

They will guarantee absolute independence with the entities that provide training to the candidates to obtain the certification.

They will make known the content of this code of ethics.

ARTICLE V. RELATIONS WITH CLIENTS

In their relationships with clients, interested entities:

They will make known the content of this code of ethics.

They will act ethically, with integrity, in good faith and professionally, aiming to achieve a high level of quality in the provision of their services, seeking the development of relationships based on trust, security and mutual respect.

They will always safeguard independence, avoiding that their professional performance is influenced by economic, family and friendship ties with clients, or their professional relationships outside of the activity of the CIs, and should not accept gifts or favors of any nature from the party. of these or their representatives.

They will not make or accept, directly or indirectly, any payment or service of greater value or different from that established for the service provided.

They will inform the client of any situation that may give rise to a conflict of interest in the provision of their services before assuming a professional assignment.

They will not carry out any promotional activity (advertising, informative material, or other) that may lead customers to an incorrect interpretation of the meaning of the Accreditation under the AEPD-DPD Scheme, or to expectations that do not respond to the real situation.

They will not offer the training required in the AEPD-DPD Scheme or advertise, on their website, or in other media, courses related to the AEPD-DPD Scheme.

They will not offer offers, discounts or other benefits to candidates to obtain the DPD certification because they come from certain training programs.

ARTICLE VI. RELATIONSHIP WITH PUBLIC AUTHORITIES AND BODIES

Relations with institutions, agencies and public administrations (state, regional and local), especially with the AEPD, will be developed under the principle of maximum collaboration and scrupulous compliance with its resolutions. The communications, requirements and requests for information that the interested entities receive from authorities and public bodies must be attended to with diligence, within the established deadlines for this.

ARTICLE VII. CODE APPLICATION CONTROL

The Certification and Training Entities will allow ENAC and the AEPD access to the registry of claims related to the ethical code and will fully collaborate with any action or investigation on compliance carried out by ENAC or the AEPD.

ARTICLE VIII. ACCEPTANCE AND INTERPRETATION OF THE CODE OF ETHICS

The AEPD-DPD Scheme requires interested entities a high level of commitment to comply with the code of ethics.

Interested entities undertake to sign and apply this code of ethics that is part of the AEPD-DPD Scheme.

Any questions that may arise about the interpretation or application of the ethical code should be consulted with the AEPD, who has the obligation to promote knowledge and compliance with the code and interpret it in case of doubt.

ARTICLE IX. BREACH OF THE CODE OF ETHICS

Failure to adhere to the code of ethics, or failure to comply with any of the commitments that it implies, will lead to the termination of the contract for the use of the Brand.

ARTICLE X. TRANSITORY REGIME

Interested entities and those that are already accredited as Certification Entities by ENAC, and Training Entities must sign the code of ethics within the terms established in the Transitory Provision of the Scheme (section 10 of the Scheme).

ANNEX IV

CODE OF ETHICS FOR PERSONS CERTIFIED AS DATA PROTECTION DELEGATES ACCORDING TO THE SCHEME OF THE SPANISH AGENCY DATA PROTECTION

PREAMBLE

This Code constitutes an express declaration of the values, principles and standards that should guide the conduct of persons certified as Data Protection Delegates (DPD), in accordance with the Certification Scheme of the Spanish Data Protection Agency (AEPD), in the exercise of their functions or tasks, and in their relationships with other employees, such as with clients, suppliers, public and private institutions, external collaborators and society in general.

Therefore, the Code of Ethics includes a set of commitments of integrity, impartiality, legality, confidentiality and transparency that must inevitably subscribe, as well as know and disseminate, those who intend to develop their professional activity as Certified Data Protection Delegates in accordance with the Scheme of the AEPD.

In this way, through this Code, it is intended to prevent the commission of behaviors contrary to the criteria it contains, while designing monitoring and control mechanisms that guarantee their full compliance by all those who carry out their professional work. as DPD certified by the AEPD Scheme.

The conduct criteria included in this Code are not intended to contemplate all situations or circumstances that the aforementioned professionals may encounter, but rather to establish general guidelines of conduct that guide them in their way of acting during the performance of their professional activity.

ARTICLE I. SCOPE OF APPLICATION

The principles, values and criteria contained in this Code of Ethics are mandatory for Data Protection Delegates certified by certification bodies accredited by the National Accreditation Company (ENAC) in accordance with the AEPD Scheme.

ARTICLE II. GENERAL PRINCIPLES

The DPDs certified in their professional activity in accordance with the AEPD scheme will carry out all their actions subject to the following principles:

Legality and integrity, Strictly complying with current legislation, in particular that referring to the provision of the service, in order to prevent any illegal activity from being carried out.

Professionalism, performing their duties with due diligence and professional rigor, and keeping their professional capacity and personal training permanently updated; They must behave before people, companies, entities and clients in a scrupulously loyal manner and independent of the limitations of any nature that may influence their own work and that of the staff for whom, eventually, they are responsible.

Responsibility in the development of their professional and personal activity, assuming only those activities that they reasonably expect to complete with the necessary skills, knowledge and competencies.

Impartiality, acting objectively without accepting the influence of conflicts of interest or other circumstances that could question the professional integrity and that of the organization to which it belongs.

Transparency, informing all interested parties in a clear, precise and sufficient manner of all the aspects that come together in the professional practice, as long as they are not subject to the confidentiality regime, in which case they will be reserved and cannot be disclosed.

Confidentiality, respecting and keeping the necessary protection and reservation of the information to which it may have access due to professional activity, safeguarding the rights of all interested parties to their privacy. Such information should not be used for personal gain or disclosed to inappropriate parties.

ARTICLE III. RELATIONS WITH THE ORGANIZATION STAFF

In its relations with the rest of the employees, managers and collaborators of the organization, the Data Protection Delegate:

You must treat the other employees or managers of your organization fairly and respectfully.

They will assume responsibility for their actions and that of their collaborators, promoting their professional development through motivation, training and communication. In any case, the relationship with collaborators must be governed by mutual respect and quality in management.

You must reject any manifestation of physical, psychological, moral harassment or abuse of authority, as well as any other conduct contrary to creating a pleasant, healthy and safe work environment.

He will ensure that the personnel under his charge do not carry out illegal activities or conduct contrary to this Code of Ethics.

It will always provide all the information necessary for the proper monitoring of the activity, without hiding errors or non-compliances, and trying to correct any deficiencies that are detected.

ARTICLE IV. RELATIONSHIPS WITH EXTERNAL COLLABORATORS AND SUPPLIERS

In its relations with external collaborators and suppliers, the Data Protection Delegate:

Establish relationships based on trust, respect, transparency and mutual benefit.

It will act with impartiality and objectivity in the selection processes of this personnel, applying criteria of competence, quality and cost, avoiding at all times the collision of interests. The contracting of services or the purchase of goods must be carried out with total independence of decision and regardless of any personal, family or economic relationship, which may cast doubt on the criteria followed in the selection.

ARTICLE V. RELATIONS WITH CLIENTS

In its relations with clients, the Data Protection Officer:

It will make known the content of this code of ethics.

It will act in an upright and professional manner, aiming to achieve a high level of quality in the provision of its services, seeking the long-term development of relationships based on trust and mutual respect.

They will always safeguard independence, avoiding that their professional performance is influenced by economic, family and friendship ties with clients, or their professional relationships outside the scope of activity as DPD, not having to accept fees, gifts or favors of any nature from part of these or their representatives.

You will not make or accept, directly or indirectly, any payment or service of more value other than that freely agreed with your employer.

He will inform the client of any conflict of interest that may exist in his professional service related to the certification, before assuming a professional assignment.

It will not carry out any promotional activity (advertising, informative material, or other) that may induce clients to misinterpret the meaning of the certifications under the AEPD Scheme, or to expectations that do not respond to the real situation.

It will provide clients with a form to formalize any complaint related to the services provided, which will be sent both to the certified person or organization affected by the complaint, as well as to the Certification Entity.

ARTICLE VI. COLLABORATION WITH CERTIFICATION BODIES

The DPDs will cooperate fully with any formal investigation into violations of this code initiated by the Certification Entities or to resolve specific cases of claims and / or complaints.

For this purpose, they must keep a record of all claims filed against them, for the activity carried out within the scope of validity of the certification and allow the

Certification Entity access to these records. Within ten days of receiving the claim, they must send a written communication and a copy of the claim to the Certification Entity.

ARTICLE VII. RELATIONSHIP WITH PUBLIC AUTHORITIES AND ADMINISTRATIONS

Relations with institutions, agencies and public, state, regional and local administrations, especially with the Control Authority, will be developed under criteria of maximum collaboration and scrupulous compliance with their resolutions. Communications, requirements and requests for information must be dealt with diligently, within the established deadlines for this.

ARTICLE VIII. PERFORMANCE OF OTHER PROFESSIONAL ACTIVITIES

The DPDs will not carry out direct or indirect competitive activities against the AEPD and / or the Certification Entity.

For this purpose, they will inform their organization of the exercise of any other work, professional or business activity, paid or not, that takes place within or outside working hours, or their significant participation as a partner in companies or private businesses, for the purposes of evaluate if they are compatible with the development of their activity or with the aims or objectives of the organization.

ARTICLE IX. ACCEPTANCE AND INTERPRETATION OF THE CODE OF ETHICS

The subjects included in the scope of this Code have a duty to know and comply with it, so they must know its content and have initialed it. The AEPD Scheme requires DPDs to have a high level of commitment to comply with this Code of Ethics.

Any questions that may arise about the interpretation or application of this document should be consulted with the Certification Entity, who has the obligation to promote knowledge and compliance with the Code and interpret it in case of doubt.

ARTICLE X. BREACH OF THE CODE OF ETHICS

Failure to comply with any of the principles, values and criteria contained in this Code may lead to an investigation of the conduct of the certification holder and, ultimately, disciplinary measures by the corresponding certification body that may lead to the suspension or withdrawal of the certification.

ANNEX V

SCHEME PROGRAM / AGENDA

CONTENT

1. Domain 1. GENERAL REGULATIONS ON DATA PROTECTION.

(Syllabus percentage: 50%)

1.1. Normative context.
1.1.1. Privacy and data protection in the international scene.
1.1.2. Data protection in Europe.
1.1.3. Data protection in Spain.
1.1.4. Standards and good practices.
1.2. The European Data Protection Regulation and Organic Law 3/2018, of December 5, on the protection of personal data and guarantee of digital rights. Fundamentals.
1.2.1. Area of application.
1.2.2. Definitions.
1.2.3. Obliged subjects.
1.3. The European Data Protection Regulation and Organic Law 3/2018, of December 5, on the protection of personal data and guarantee of digital rights. LOPD. Beginning
1.3.1. The right / duty pairing in data protection.
1.3.2. Legality of the treatment
1.3.3. Loyalty and transparency
1.3.4. Purpose limitation
1.3.5. Data minimization
1.3.6. Accuracy
1.4. The European Data Protection Regulation and Organic Law 3/2018, of December 5, on the protection of personal data and guarantee of digital rights. Legitimation
1.4.1. Consent: granting and revocation.
1.4.2. Informed consent: purpose, transparency, conservation, information and duty of communication to the interested party.
1.4.3. Children's consent.
1.4.4. Special categories of data.
1.4.5. Data related to criminal offenses and convictions.
1.4.6. Treatment that does not require identification.
1.4.7. Legal bases other than consent. Rights
1.5. of individuals.

1.5.1. Transparency and information
1.5.2. Access, rectification, deletion (oblivion).
1.5.3. Opposition
1.5.4. Automated individual decisions.
1.5.5. Portability.
1.5.6. Limitation of treatment.
1.5.7. Exceptions to rights.

1.6. The European Data Protection Regulation and Organic Law 3/2018, of December 5, on the protection of personal data and guarantee of digital rights. Compliance measures.

1.6.1. Data protection policies.
1.6.2. Legal position of the parties. Managers, co-managers, managers, sub-manager of the treatment and their representatives. Relations between them and formalization.
1.6.3. The registration of processing activities: identification and classification of data processing.

1.7. The European Data Protection Regulation and Organic Law 3/2018, of December 5, on the protection of personal data and guarantee of digital rights. Proactive responsibility.

1.7.1. Privacy by design and by default. Fundamental principles.
1.7.2. Impact assessment related to data protection and prior consultation. High-risk treatments.
1.7.3. Personal data security. Technical and organizational security.
1.7.4. Security violations. Notification of security breaches.
1.7.5. The Data Protection Officer (DPD). Regulatory framework.
1.7.6. Codes of conduct and certifications.

1.8. The European Data Protection Regulation. Data Protection Delegates (DPD, DPO, or Data Privacy Officer).

1.8.1. Designation. Decision-making process. Formalities in the appointment, renewal and dismissal. Analysis of conflict of interest.
1.8.2. Obligations and responsibilities. Independence. Identification and report to management.
1.8.3. Procedures Collaboration, prior authorizations, relationship with interested parties and claims management.
1.8.4. Communication with the data protection authority.
1.8.5. Professional competence. Negotiation. Communication. Budgets.
1.8.6. Training.
1.8.7. Personal skills, teamwork, leadership, team management.

1.9. The European Data Protection Regulation and Organic Law 3/2018, of December 5, on the protection of personal data and guarantee of digital rights. International data transfers

1.9.1. The adequacy decision system.
1.9.2. Transfers through adequate guarantees.
1.9.3. Binding Corporate Rules
1.9.4. Exceptions
1.9.5. Authorization of the supervisory authority.
1.9.6. Temporary suspension
1.9.7. Contractual clauses

1.10. The European Data Protection Regulation and Organic Law 3/2018, of December 5, on the protection of personal data and guarantee of digital rights. Control Authorities.

1.10.1. Control Authorities.
1.10.2. Powers.
1.10.3. Sanctions regime.
1.10.4. European Committee for Data Protection.
1.10.5. Procedures followed by the AEPD.
1.10.6. Jurisdictional protection.
1.10.7. The right to compensation.

1.11. GDPR interpretation guidelines.

1.11.1. GT guides art. 29.
1.11.2. Opinions of the European Data Protection Committee
1.11.3. Criteria of jurisdictional bodies.

1.12. Sectoral regulations affected by data protection.

1.12.1. Health, Pharmaceutical, Research.
1.12.2. Protection of minors
1.12.3. Equity Solvency
1.12.4. Telecommunications
1.12.5. Video surveillance
1.12.6. Insurance
1.12.7. Advertising, etc.

1.13. Spanish regulations with data protection implications.

1.13.1. LSSI, Law 34/2002, of July 11, on services of the information society and electronic commerce
1.13.2. LGT, Law 9/2014, of May 9, General Telecommunications
1.13.3. Law firm-e, Law 59/2003, of December 19, of electronic signature

1.14. European regulations with data protection implications.

1.14.1. E-Privacy Directive: Directive 2002/58 / EC of the European Parliament and of the Council of July 12, 2002, on the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) or e-Privacy Regulation when approved.

1.14.2. Directive 2009/136 / EC of the European Parliament and of the Council, of November 25, 2009, amending Directive 2002/22 / EC on universal service and the rights of users in relation to networks and services of electronic communications, Directive 2002/58 / EC on the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No. 2006/2004 on cooperation on consumer protection .

1.14.3. Directive (EU) 2016/680 of the European Parliament and of the Council of April 27, 2016 on the protection of natural persons with regard to the processing of personal data by the competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offenses or execution of criminal sanctions, and the free circulation of said data and by which the Framework Decision 2008/977 / JAI of the Council is repealed.

2. Domain 2. ACTIVE LIABILITY.

(Syllabus percentage: 30%)

2.1. Analysis and risk management of personal data processing.

2.1.1. Introduction. General framework for risk assessment and management. General concepts.

2.1.2. Risks evaluation. Inventory and valuation of assets. Inventory and assessment of threats. Existing safeguards and assessment of their protection. Resulting risk.

2.1.3. Risk management. Concepts. Implementation. Selection and assignment of safeguards to threats. Protection assessment. Residual risk, acceptable risk and unacceptable risk.

2.2. Risk analysis and management methodologies.

2.3. Compliance program for Data Protection and Security in an organization.

2.3.1. The Design and implementation of the data protection program in the context of the organization.

2.3.2. Objectives of the compliance program.

2.3.3. Accountability: The traceability of the compliance model.

2.4. Security of the information.

2.4.1. Regulatory framework. National Security Scheme and NIS directive: Directive (EU) 2016/1148 relating to measures designed to guarantee a high common level of security for networks and information systems in the Union. Scope of application, objectives, main elements, basic principles and minimum requirements.

2.4.2. Cybersecurity and information security governance. Generalities, Mission, effective governance of Information Security (IS). SI concepts. Scope. IS government metrics. State of the SI. SI strategy.

2.4.3. Implementation of information security. Security by design and by default. The life cycle of Information Systems. Integration of security and privacy in the life cycle. Quality control of the IS. Data Protection Impact Assessment

2.5. "EIPD".

2.5.1. Introduction and fundamentals of the DPIA: Origin, concept and characteristics of the DPIA. Scope and need. Standards.

2.5.2. Carrying out an impact assessment. Preparatory and organizational aspects, analysis of the need to carry out the evaluation and prior consultations.

3. Domain 3. TECHNIQUES TO GUARANTEE COMPLIANCE WITH THE DATA PROTECTION REGULATIONS.

(Syllabus percentage: 20%)

3.1. The data protection audit.

3.1.1. The audit process. General questions and approach to the audit. Basic characteristics of the Audit.

3.1.2. Preparation of the audit report. Basic aspects and importance of the audit report.

3.1.3. Execution and monitoring of corrective

3.2. actions. Information Systems Audit.

3.2.1. The Role of Auditing in Information Systems. Basic concepts. IS Audit Standards and Guidelines.

3.2.2. Internal control and continuous improvement. Good practices. Integration of the data protection audit in the IS audit.

3.2.3. Planning, execution and monitoring.

3.3. The management of the security of the treatments.

3.3.1. National Security Scheme, ISO / IEC 27001: 2013 (UNE ISO / IEC 27001: 2014: Information Security Management System Requirements, ISMS).

3.3.2. Asset Security Management. Logical and procedural security. Security applied to IT and documentation.

3.3.3. Disaster Recovery and Business Continuity. Protection of technical and documentary assets. Planning and management of Disaster Recovery.

3.4. Other knowledge.

3.4.1. The cloud computing.

3.4.2. Smartphones.

3.4.3. Internet of things (IoT).

3.4.4. Big data and profiling.

3.4.5. Social networks

3.4.6. User tracking technologies

3.4.7. Blockchain and latest technologies

ANNEX VI

PROCEDURE FOR THE SELECTION AND APPOINTMENT OF EVALUATORS

The evaluator is the professional with knowledge and professional experience equivalent to or higher than the candidate to be certified as DPD, and with the capacity to initially evaluate the exams, as well as the allegations that the candidates present during their completion. Their work cannot compromise the principles of independence and impartiality that govern assessment and certification tasks. An evaluator is considered to meet the conditions if he is certified under this AEPD-DPD Scheme.

The evaluators may be the entity's own personnel or may be contracted, in which case, for any questions that may arise regarding the breach of their commitments in relation to the Scheme, they will adjust to what is indicated in the contract.

The selection procedure defines the criteria relating to the selection and maintenance of the companies or people hired.

1. Requirements of the evaluators.

Candidate evaluators must meet the following requirements.

a) University degree qualification.

b) Experience of at least five years in the field of data protection and / or information security.

2. Merits.

The following merits will be assessed:

3.1. Preferential merits.

1. University qualification higher than the undergraduate: doctorate, postgraduate or master's degree in the field of data protection and / or information security.

2. Teaching experience in degrees related to data protection or information security.

3. To be in possession during the last five years of certifications related to data protection or information security.

3.2. Additional merits.

The following merits will also be assessed:

1. Experience of more than five years in the field of data protection or information security.
2. Participation in national or international standardization committees related to data protection or information security.
3. Publication of articles related to both subjects.

3. Incompatibilities and exclusions.

Those people who could see their independence and impartiality compromised by any professional, family or personal circumstance may be partially or totally excluded from the evaluation process.

4. Functions of the evaluator.

The evaluator is responsible for:

1. Evaluate in an impartial and confidential manner the documentation presented by the candidates and the tests to which they are submitted. The assessment of the exam will be done without knowing the identity of the candidate.
2. Issue a report with the result of the evaluation.

In addition, it corresponds to:

1. Inform the Certification Entity of any professional, family or other relationship that may affect the objectivity and impartiality of its evaluation work.
2. Assess the reasoned challenge of any candidate for transfer to the Certification Entity.

5. Selection procedure.

The Certification Entity will evaluate the candidacies of the evaluators and will resolve by communicating its decision to the candidate.

6. Selection committee.

The Certification Entity will create an internal body subject to the internal regulations and the Scheme to select the evaluators.

7. Records and work procedures.

The CVs of all the evaluators will be kept on file, in which the records on qualifications, training and experience that demonstrate their adequate technical competence are kept.

Likewise, copies of those quality system documents that are applicable to their work, and especially all the procedures and formats applicable to the evaluation activity, will be distributed in a controlled manner to the evaluators.

ANNEX VII

EXAM RESULT REPORT MODEL

The exam is passed with a result equal to or greater than 75% of the correct answers, and at least 50% in each of the domains. Its results have been:

DOMAIN	Punctuation minimal	Punctuation obtained
1 - General Data Protection Regulations 2 -	38	<N1>
Active Responsibility	2. 3	<N2>
3 - Techniques to Ensure Compliance with the Data Protection Regulations and Other Knowledge	fifteen	<N3>

MINIMUM SCORE TO BE SUITABLE	113
SCORE OBTAINED	X
OUTCOME:	SUITABLE / NOT SUITABLE

In the case of the unfit, send the information on the distribution of errors by headings:

Epigraphs Involved	No. of errors
1.1	
1.2	
1.3	
1.4	
1.5	
1.6	
1.7	
1.9	
1.10	
1.11	

1.14	
2.1	
2.2	
2.3	
2.4	
2.5	
3.1	
3.2	
3.3	
3.4	

ANNEX VIII

CONTENT OF THE CERTIFICATION OF CONFORMITY WITH THE SCHEME OF THE SPANISH AGENCY FOR DATA PROTECTION OF DELEGATE OF DATA PROTECTION

Each Certifying Entity may freely have its own Certification of Conformity format with the AEPD Scheme of Data Protection Delegate, which must show, at least, the following content:

- Logo of the Certifying Entity.

- Identification of the Certifying Entity.

- Mark of the Certification Scheme of Data Protection Delegates

- Text: "Certificate of Conformity with the Certification Scheme of Delegate of Data Protection of the Spanish Agency for Data Protection ".

- Text: "« Certifying Entity »certifies that the candidate reviewed has been evaluated and found in accordance with the requirements of the Certification Scheme for Data Protection Delegates of the Spanish Data Protection Agency: "

- "Identify with name, surname and DNI the person who is the object of the certification".

- Text: "Certificate number:« certificate number »".

- Text: "Date of initial certification of conformity:" day "of" month "of" year ".

- Text: "Date of renewal of the certificate of conformity:" day "of" month "of" year "".

- Text: "Expiration date of the certificate of conformity:" day "of" month "of" year "".

- Text: "Date:« Locality (whichever corresponds) »,« day »of« month »of« year »".

- Signature: Name and Surname of the competent person in charge of the Certifying Entity.

The texts that appear between angle brackets will be adapted to the specific aspects of the certification issued.

Below is an illustrative model of the aforementioned Certification of Conformity.

Logo of the Certifying Entity with brand accreditation

MARK OF THE SCHEME CERTIFICATION OF DELEGATES OF DATA PROTECTION

Certification of Conformity with the Scheme of the Spanish Agency for Data Protection of Delegate of Data Protection

Certifying Entity may freely have its own Certification of Conformity format with the AEPD Scheme of Data Protection Delegate, which must show, at least, the following content:

- Logo of the Certifying Entity.

- Identification of the Certifying Entity.

- Mark of the Certification Scheme of Data Protection Delegates

- Text: "Certificate of Conformity with the Certification Scheme of Delegate of Data Protection of the Spanish Agency for Data Protection ".

"Certifying Entity" certifies that the candidate reviewed has been evaluated and found to be in accordance with the requirements of the Certification Scheme for Data Protection Delegates of the Spanish Agency for Data Protection, as indicated in the corresponding Certification Report of "date " for:

«Identify with name, surname and DNI the person who is the object of the

certification». "Date of initial certification of conformity:" day "of" month "of" year "

"Date of renewal of the certification of conformity:" day "of" month "of" year ""

"Certificate number:" certificate number "

"Date:« Locality (whichever corresponds) »,« day »of« month »of« year »

Signature: "Name and Surname of the competent person in charge of the Certifying Entity"

Signature of the person in charge of the Certifying Entity

Full name / business name of the Certifying Entity and website.

Postal / electronic address

Postal Code, Province, Country.

CERTIFICATION SCHEME FOR DATA PROTECTION DELEGATES OF THE SPANISH PROTECTION AGENCY OF DATA (AEPD-DPD SCHEME)