CERTIFICATION SCHEME OF DATA PROTECTION OFFICERS FROM THE SPANISH DATA PROTECTION AGENCY (DPO-AEPD SCHEME).

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

CERTIFICATION SCHEME OF DATA PROTECTION OFFICERS FROM THE SPANISH DATA PROTECTION AGENCY (DPO-AEPD SCHEME).

Written by Assessment and Technological Studies Unit of the Spanish Data Protection Agency.
October 2, 2017. Version 1.1

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

Índice

1. PURPOSE

The purpose of this document is to establish the general guidelines that regulate the Certification Scheme for Persons for the "Data Protection Officer" category, set out in Section 4 of Chapter IV of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and the relationships between the different Agents who will be involved in such certification under conditions of accreditation.

Certification of persons is a valid tool for the objective, impartial assessment of the competence of an individual to carry out a specific activity. The subsequent public statement made by the certifier provides the market with useful, verified information on the criteria applied to individuals in order to obtain professional certification. The validity and term of the rules of this Scheme are ensured through the active participation of experts and representatives of the different parties interested in its development.

The technical competence of the certification bodies involved and their alignment with the requirements established by the Scheme, as well as their systematic and impartial behaviour, is achieved through their accreditation by the National Accreditation Body (hereinafter ENAC), in accordance with the requirements of international regulations for the certification of persons.

The Spanish Data Protection Agency (hereinafter AEPD), as the owner of the Scheme, is responsible for its development and review, and actively involves the various interested parties in both processes. It does so through a Technical Committee which is subject to an operational Regulation that ensure both the equitable representation of all parties involved, as well as periodic meetings to analyse and assess the progress of the work and tasks of the Data Protection Officer (DPO), and of their compliance with competency requirements and assessment schemes.

Through the aforementioned Committee, the AEPD defines the criteria for recognising entities that may perform the compliance assessment (certification), which is aimed at making it possible to award the "Mark of Conformity" associated with the DPO Certification Scheme promoted by the AEPD, which exclusively and unequivocally identifies those persons who have demonstrated their competence to carry out the tasks of the DPO.

1.1. REFERENCES

- UNE-EN ISO/IEC 17024:2012. Conformity Assessments. General requirements for bodies operating certification of persons.
- Regulation (EU) 2016/679 of the European Parliament and of the Council, of 27 April 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
- Organic Law of Protection of Personal Data.
- Regulation Implementing the Organic Law of Protection of Personal Data.

All of the aforementioned documents are applicable in their most recent valid version.

1.2. ACRONYMS

- DPO: Data Protection Officer
- DPO-AEPD Scheme: Certifying Scheme of DPO from AEPD
- RGPD: General Data Protection Regulation
- LOPD: Organic Law of Protection of Personal Data
- RLOPD: Regulation Implementing the Organic Law of Protection of Personal Data.

2. SCHEME AGENTS

- **The AEPD**, as the owner of the Scheme, is responsible for promoting its development, review, and continuous validation, and authorises the other agents to actively participate in said scheme.
- **The National Accreditation Body (ENAC).** It is designated by the AEPD as the single entity authorised to accredit certification bodies that would like to participate in the Scheme, and takes into consideration both the requirements of the UNE-EN ISO/IEC 17024:2012 standard, as well as the specific requirements set out by the Scheme.
- **Certification Bodies (CB).** They offer the certification (only under ENAC accreditation and in accordance with the requirements of the Scheme and UNE-EN ISO/IEC 17024:2012 standard) for the "Data Protection Officer" category. As part of the process, they may receive the rights of use and rights to license the use of the "Mark of Conformity" to certified persons, according to the terms set out in section 3.

  The authorisation of a Certification Body by the AEPD shall be subject to obtain and maintain the accreditation, which may be rescinded if:

- ENAC withdraws the CB's accreditation to operate under this Scheme.
- The CB fails to comply with the rules of use for marks or does not comply with its obligation to monitor their use by the certified persons.
- The CB fails to comply with any of the other rules established by the AEPD.

- **Training entities (TE).** These are the entities that offer training which satisfies the requirements for obtaining this certification. As necessary, the AEPD may establish a public, non-discriminatory process for authorising TEs. If needed, a list of requirements for both the training courses as well as the entities offering such courses will be published, establishing the content, minimum duration of training and requirements regarding training personnel, resources, facilities, performance, etc.

  Training Entities must request Certification Bodies to recognize their training programmes in accordance with the requirements established in section 6.3.

3. MARK OF THE SCHEME

So that the market can identify Data Protection Officers certified according to the AEPD Scheme, the AEPD has created a Mark of conformity with the Scheme (hereinafter, the Mark of the Scheme). The AEPD may cede the rights to its use to any of the Scheme's agents in accordance with specific rules.

Annex II.A contains the rules of use of the Mark and **Annex II.B** the contract model for the use of the Mark.

The agents identified in section 2 may use the Mark of the Scheme exclusively to indicate such status, once authorisation has been received by the AEPD and as long as that authorisation remains valid. They must comply with the applicable rules of use for the Mark at all times.

Any use or concession of use of the Mark of the Scheme, as well as limitations on such use, will be regulated through specific references in the "contracts" signed between the AEPD and the agent.

4. SCHEME COMMITTEE

The AEPD is responsible for developing, reviewing, and periodically validating the DPO Certification Scheme at least once every five years, or before if conditions merit such a review. To do so, it has created and maintains a DPO Certification Scheme Committee (hereinafter, the Scheme Committee), as a means of contacting and involving the various parties interested in the certification of persons to carry out the functions of a Data Protection Officer. Interested parties

will be continuously involved in the aforementioned Committee to validate and maintain the Scheme.

In addition to the AEPD as the owner of this Committee, the Scheme Committee will comprise the interested entities, organisations and associations.

Its organisation and operation are governed by its internal Regulations.

5. AUTHORISATION OF CERTIFICATION BODIES

The recognition or designation of certification bodies that may offer and perform certification of persons in accordance with the DPO-AEPD Scheme is based on the criteria and requirements established by this Scheme.

This recognition is based on, but not limited to, technical competence to certify, and therefore the body must obtain and maintain accreditation by ENAC to certify persons as Data Protection Officers with the Agency Scheme (DPO -AEPD Scheme).

The participation of ENAC to provide accreditation ensures that exclusively those entities that have demonstrated their technical competence to perform this specific function in accordance with internationally accepted criteria are designated as certification bodies.

Furthermore, this designation by AEPD is strictly aimed at informing those persons who are potentially interested in becoming certified as “Data Protection Officers” which entities perform this certification in accordance with the requirements set out by the AEPD and its Scheme Committee.

The AEPD will maintain an updated registry of authorised certification bodies, which will include the following information provided by ENAC: name, authorisation number, date authorised.

Authorised certification bodies are responsible for informing AEPD of any important change to their accreditation status, such as the suspension or withdrawal of accreditation by ENAC, which may affect recognition requirements.

The AEPD will continuously verify that these entities comply with the obligations arising from the recognition and use of the Mark of Conformity, whether through its own actions or through information provided by certified persons and companies that are the final users of the “Data Protection Officer” certification.

In order to facilitate a way to acquire experience using the Scheme, certification bodies may request and be subject to a provisional designation, which may not be renewed and will have a maximum term of one year. This provisional authorisation will be subject to submitting an accreditation application to ENAC and successful completion of the application review process. During this first year of provisional designation, at least two certification exams must be held.

During the term of the provisional designation, the certification body may, with the sole purpose of facilitating access to certification for interested persons and thus acquiring the necessary experience, use its status as a provisionally designated certification body by the Scheme; however, it may not use any of the Scheme marks (from ENAC and AEPD). If, a year after the provisional designation was granted to the certification body, it has not obtained accreditation from ENAC, and provided that this was due to reasons attributable to the certification body, the provisional designation will automatically expire.

6. DATA PROTECTION OFFICER CERTIFICATION SCHEME

The Scheme establishes the competence requirements for persons who perform the function of Data Protection Officer, as well as the criteria to evaluate whether candidates possess that competence, so that when the result of that process is favourable, the certification body can issue a statement of compliance or certificate.

6.1. PROFILE OF THE DATA PROTECTION OFFICER.

The DPO is a professional whose tasks are set out in Article 39 of Regulation (EU) 679/2016, and who is responsible for applying legislation on privacy and data protection**.**

The data protection officer will perform at least the following tasks:

a) inform and advise the controller or the processor and the employees who process data of the obligations incumbent upon them under the Regulation and other data protection provisions in the European Union or Member States;
b) supervise compliance with the provisions of the Regulation and other data protection provisions in the European Union or Member States and with the policies of the controller or processor in relation to the protection of personal data,
c) supervise the assignment of responsibilities,
d) supervise awareness raising and training of personnel who participate in processing operations
e) supervise the corresponding audits;
f) offer advice requested regarding data protection impact assessments

g) supervise their application in accordance with article 35 of the Regulation;
h) cooperate with the supervisory authority;
i) act as the contact point for the supervisory authority for issues regarding data processing, including the prior consultation referenced in Article 36, and
j) consult with the supervisory authority, as appropriate, on any matter.

The data protection officer will carry out their functions by paying due attention to the risks associated with data processing operations, and keeping in mind the nature, scope, context, and purposes of data processing.

To do so, he/she must be able to:

a) collect information to identify processing activities,
b) analyse and check the compliance of processing activities, and
c) inform, advise, and issue recommendations to the controller or the processor.
d) collect information to supervise the register of processing operations.
e) provide advice on the application of the principle of data protection by design and by default.
f) advise on:
    - whether a data protection impact assessment should be carried out or not
    - what methodology should be followed when carrying out a data protection impact assessment
    - whether a data protection impact assessment should be carried out in-house or outsource it
    - what safeguards (including technical and organisational measures) to apply in order to mitigate any risk to the rights and interests of the data subjects
    - whether or not the data protection impact assessment has been carried out correctly
    - if its conclusions (whether to continue with the processing or not and what safeguards should be applied) are in compliance with the Regulation.
g) prioritise their activities and focus their efforts on those issues which pose a greater risk in terms of data protection.
h) advise the data controller on:
    - which methodology should be used when carrying out a data protection impact assessment,
    - which areas should be subject to an internal or external data protection audit,
    - which internal training activities to provide to personnel or the managers responsible for data processing activities and to which processing operations the most time and resources should be dedicated.

6.2. REQUIRED COMPETENCES TO THE DATA PROTECTION OFFICER.

The DPO must have experted knowledge of data protection aw and practices. Therefore, we have identified the knowledge, skills, and abilities that the person to be certified must know or have to carry out the tasks of the Data Protection Officer.

These generic functions of the DPO can be summed up as advising and supervision tasks in the following areas, among others:

1. Compliance with principles relating to processing , such as purpose limitation, data minimisation or accuracy
2. Identifying the legal basis for data processing
3. Assessment of the compatibility of purposes other than those which gave rise to initial data collection
4. Determining whether any sectoral regulation may determine specific data processing conditions that are different from those established by general data protection regulations
5. Designing and implementing measures to provide information to data subjects
6. Establishing mechanisms to receive and manage requests to exercise rights of the data subjects
7. Assessing requests to exercise rights of the data subjects
8. Hiring data processors, including the content of the contracts or legal documents that regulate the controller – processor relationship
9. Identifying international data transfer instruments that are suited to the needs and characteristics of the organisation and the reasons that justify the transfer
10. Design and implementation of data protection policies
11. Data protection audits
12. Establishing and managing a register of processing activities
13. Risk analysis of the processing operations carried out
14. Implementing data protection measures by design and by default that are suited to the risks and nature of the processing operations
15. Implementing security measures that are suited to the risks and nature of the processing operations
16. Establishing procedures to manage violations of data security, including assessing the risk to the rights and freedoms of the data subjects and procedures to notify supervisory authorities and the data subjects
17. Determining the need to carry out data protection impact assessments
18. Carrying out data protection impact assessments
19. Relations with supervisory authorities
20. Implementing training and awareness programmes for personnel on data protection.

6.3. PRE-REQUISITES.

To reach the assessment phase, candidates must meet one of the following pre-requisites:

1) Demonstrate professional experience of at least five years on projects and/or activities and tasks related to DPO functions regarding data protection.

2) Demonstrate professional experience of at least three years on projects and/or activities and tasks related to DPO functions regarding data protection, and at least 60 hours of recognized training on subjects related to the programme.

3) Demonstrate professional experience of at least two years on projects and/or activities and tasks related to DPO functions regarding data protection, and at least 100 hours of recognized training on subjects related to the programme.

4) Demonstrate at least 180 hours of recognized training on subjects related to the programme.

The recognition of training programmes will be made according to several requirements: duration required, subject taught according to the program defined in the Scheme, validation method by passing a test (it is not enough to justify attending training) and teaching methodology that includes teaching theoretical knowledge, practical exercises and teamwork exercises.

The distribution of the hours of training programmes will follow the same percentage established for each one of the domains of the program of the Scheme.

Training entities will request certification bodies to recognize the training programmes they provide in accordance with the above requirements.

If a candidate does not have the experience required, up to one year of experience may be recognised by demonstrating additional qualifications.

Training and experience acquired nationally and in the European Union will be recognised.

The assessment of the training and experience required in the pre-requisites regarding the General Data Protection Regulation (RGPD) will be that adopted as of the date of entry into force of this regulation: 25/5/2016.

The conditions for demonstrating compliance with the pre-requisites are set out in **Annex I** of this Scheme.

6.4. CODE OF ETHICS.

For the purposes of demonstrating integrity and the high level of professional ethics with which DPO candidates must comply, a document has been created outlining this commitment, whose content is explained in **Annex III**.

The Code of Ethics must be accepted by the candidate before they can be awarded the certificate.

6.5. ASSESSMENT METHOD.

The assessment process is based on both the valuation of knowledge and experience, as well as ongoing professional development.

Through the corresponding assessment tests, the candidate must demonstrate that they posses adequate competence, that is, the theoretical knowledge, professional capacity and personal skills needed to carry out the tasks that correspond to the position of Data Protection Officer, under the terms and conditions established by the AEPD Certification Scheme.

6.5.1. Exam.

Knowledge and technical or professional capability will be evaluated by taking an exam, which has the following characteristics:

- The exam will test candidates on topics related to the specific knowledge indicated in the program of the Scheme detailed in section 6.5.3, in accordance with the weighting criteria established for each of the fields into which the corresponding tasks and competencies to be assessed are organised.
- The exam must be passed to obtain certification. The purpose of the exam is to assess the candidate's theoretical/practical knowledge to carry out DPO functions.
- The exam consists of 150 multiple-choice questions; 75% must be answered correctly to pass. Twenty percent of the questions, i.e. 30 questions, will describe a practical scenario (of a regulatory, organisational and technical nature) that the question will deal with.
- The questions are distributed into one of the programme fields or blocks in accordance with the following weighting:
  - Field 1 – 50%, 75 questions, 15 with a scenario.

- Field 2 – 30%, 45 questions, 9 with a scenario.
- Field 3 – 20%, 30 questions, 6 with a scenario.

- To pass the test, 50% of the questions in each block or field must be answered correctly. In other words, 75 points must be obtained by adding the minimum score from the three fields, and the rest of the points needed to obtain 75% of the total can be from any field.
- The questions will have four possible answers, of which only one is correct. Each correct answer will count as 1 point. No points are awarded for questions incorrectly anwered or left unanswered. Therefore, at least 112.5 points must be obtained in order to pass.
- The exam lasts four hours.
- The result of the assessment exam will be “pass” or “fail” for each exam call.
- Each certification body can offer the exam as often as it wishes, but must inform the AEPD of the exam date at least three months in advance.
- Notwithstanding the above, single, coordinated exam sittings can be established through an agreement by all of the certification bodies.

6.5.2. Programme or List of Contents.

The contents to be assessed in the certification exam fall into the following fields or topics according to the weighting indicated below:

Field 1 GENERAL DATA PROTECTION REGULATIONS. Compliance with European regulations, national rules, and European directive on ePrivacy. Guidelines and guides from art. 29 WG, etc.

Weight: 50%.

Field 2 ACCOUNTABILITY. Personal data processing risk assessment and management; data protection impact assessment, data protection by design, data protection by default, etc.

Weight: 30%.

Field 3 TECHNIQUES TO ENSURE COMPLIANCE WITH DATA PROTECTION REGULATIONS AND OTHER KNOWLEDGE. Security audits, data protection audits, etc.

Weight: 20%.

The contents for each topic are specified in **Annex IV.**

6.5.3. Evaluators.

The group of evaluators is comprised of independent professionals of the Scheme who have training and professional experience equivalent to or greater than the candidate to be certified, and the capability to evaluate the assessment exams. They must ensure the independence of their judgement, issuing a report with the result of the assessment, which is the basis for the decision to award the certificate to the candidate being assessed.

The evaluators who participate in the assessment process must have been designated in accordance with the process and requirements described in **Annex V.** This document also describes how evaluator activities are supervised as established by the Scheme.

6.6. CERTIFICACION CRITERIA.

6.6.1. Initial certification.

To obtain certification as a DPO, candidates must meet the pre-requisites established in section 6.3 and present the following documentation:

a) Application form.
b) Detailed CV.
c) Documentation demonstrating they meet the pre-requisites.
d) Proof of payment for the corresponding fee.

With this application the candidate states that they are aware of the certification process laid out in this document and agrees to sit the assessment tests.

Once the application has been submitted, the Certification Body will evaluate it so as to verify that all of the information is complete.

If after this initial evaluation, the information is not complete, the candidate will be informed in writing that their certification application has not been accepted. They will be given a period of 10 working days to provide any missing information. If, at the end of this period, they have not been able to correct the deficiency, the candidate will not be accepted, which will be communicated to them via written notification.

If the application is accepted, the candidate will be informed in writing.

Acceptance of the application means the candidate will be admitted to sit the assessment exam.

If the application is accepted, but not for the desired exam sitting (if there are several), the applicant will also be notified in writing.

Any decisions made by the Certification Body with regard to the acceptance process may be subject to the corresponding appeal, under the terms established in section 7 of this Scheme.

Exam sitting is understood to be the announcement of an assessment exam being held on a specific date and at a specific examination centre.

The applicant must appear in person to verify their identity and pass the exam.

When the applicant fails the assessment exam, they will be informed in writing of the result before taking the exam again, if they are entitled to re-sit the exam.

6.6.2. Grant of the certificate.

Tras superar el examen, la Entidad de Certificación concederá la certificación a los candidatos que hubieran obtenido el resultado de “apto”.

Previamente el solicitante deberá aceptar expresamente el Código Ético y las Normas de Uso de la marca del certificado.

A cada persona certificada la Entidad de Certificación le asignará un número identificativo intransferible y que será utilizado en el futuro para su identificación, junto con el número identificativo de la entidad de certificación que emitió el certificado.

En los casos en que se conceda la certificación, la Entidad de Certificación emitirá un certificado justificativo que será enviado al titular de la certificación, de acuerdo con el **Anexo VI**.

El certificado emitido tendrá un período de validez de tres años, salvo que la persona certificada sea sancionada. El período de validez comenzará a partir de la fecha de concesión del certificado.

6.6.3. Maintainance of certification.

If, during the certificate validity period, legal or technological changes occur that, in the opinion of the Scheme Committee, make it necessary to review or significantly adapt the certificate granted, the appropriate criteria may be established to maintain the validity of the certificates already granted.

6.6.4. Recertification.

The certification will be valid for three years and its recertification will require the candidate to demonstrate that they have completed:

- a minimum of 60 hours of training received and/or taught, during the period the certificate was valid, with an annual minimum of 15 hours on subjects included in the DPO certification programme, and

- at least one year of professional experience on projects and/or activities and tasks related to DPO functions regarding personal data protection and/or information security, witnessed by a third party (employer or similar party).

Teaching training will be assessed as twice the hours as receiving training. Training that does not specify its duration, the training entity, and the title of the training will not be valid. In the exceptional, justified case of not performing the annual minimum required training during one of the three years, this training may be completed in one of the two remaining years.

The recertification must be requested before the certificate expiration date.

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

If the certified person does not receive the notification from the Certification Body informing them of the end of the certificate validity, this does not exempt them from compliance with the provisions of this section.

The candidate must submit the recertification application along with a list of any claims that they may have received during the full certification period for faulty actions in the activity for which they are certified or a statement certifying that they have not received any claims. They must also submit acceptance of the Code of Ethics and the Rules of Use for the certificate mark, as well as proof of payment of the renewal fee.

Once the application has been submitted, the Certification Body will evaluate it so as to verify the validity of the documentation provided. If after this initial evaluation, the information is not complete, the candidate will be informed in writing that their recertification application has not been accepted. They will be given a maximum period of 90 calendar days to provide any missing information. If, at the end of this period, they have not been able to correct the deficiency, the candidate will be designated as not renewed,

which will be communicated to them via written notification and their certification will be withdrawn.

If the application is accepted, the candidate will be informed in writing.

If the certification is renewed, the Certification Body will issue a new certificate with the same identification number which was assigned during the first certification. The new certificate will be valid for three years.

6.7. CRITERIA FOR SUSPENSION OR WITHDRAWAL OF CERTIFICATION.

6.7.1. Temporary voluntary suspension.

If the certified person states that they no longer comply with the contractual or other requirements of the Scheme, their certificate will be suspended for a period not exceeding 12 months.

To return to certified status, the certification body must perform verifications designed to ensure that the reasons that caused the request for suspension have disappeared, provided that more than one year has not passed from the date the certification was suspended. The candidate must also provide documentation to demonstrate that they are in a position to obtain the certificate under the same terms and conditions established for renewal in the above section.

Once a year has passed from suspension of the certificate and if it has not been possible to renew it, or the reasons that caused the suspension have not disappeared, the certification will be withdrawn definitively and the candidate must re-start the entire process to obtain certification again.

6.7.2. Temporary suspension due to conduct contrary to the Scheme.

The following are causes for suspension by the certification body:

- The failure of the certified person to submit documentation, registers, or any information requested of them by the certification body to maintain said certification or to investigate a claim addressed to the person.

- Failure to perform any of the tasks or functions of the DPO, as well as the lack of competence to perform a task assigned under this Scheme.

- Any statements or uses by the person in their position as certificate-holder that exceed the scope of the certification which are deceitful or in any other manner damage or discredit the certification Scheme.
- Behaviour contrary to the Code of Ethics.
- The use of Scheme markin a manner that is not permitted or contrary to the rules of use for Scheme marks.
- Violation of any other Scheme rules that pertain to them by the certified person.

Any of these failures to comply may result in the temporary suspension of the certification for a maximum period of six months. The accumulation of three violations may result in suspension of the certification for a minimum period of six months up to half of the certification cycle, after which the certification will be withdrawn.

If, as a result of the investigation of these cases, the certification body concludes that there is evidence that the certified person no longer complies with the contractual or other requirements of the Scheme, including the possession of a specific skill, and as a result their certificate ceases to be valid, the entity may temporarily suspend the certificate unless the underlying causes are corrected.

Any penalties established will be without prejudice to civil, penal, professional or other liability that certified persons may incur in the exercise of their profession.

In order to regain certified status, the certification body must require the appropriate verifications to confirm that the causes underlying the suspension have disappeared, and they may even require partial or full re-assessment.

6.7.3. Withdrawal of certification.

The following are causes for a certification body to withdraw a certification that has already been issued:

- Any of the aforementioned causes for temporary suspension, depending on their severity or their repetition, such as the repetition of a specific type of violation that already resulted in a temporary suspension, which implies that the DPO's conduct has not been corrected.

- The suspension of the certification for a period greater than half of the certification cycle.
- The certified person's lack of cooperation to return the certificate in the event of penalisation.

To regain certified status, the person must submit themselves to the entire initial certification process. The Certification Body may require that, before undergoing the assessment process, the person demonstrate that they have resolved the causes that led to the withdrawal of the prior certificate, without this being considered discriminatory treatment.

The Certification Body reserves the right to accept new applications from professionals who have been penalised.

6.8. RIGHTS AND OBLIGATIONS OF CERTIFIED PERSONS.

6.8.1. Rights.

Certificate holders have the right to:

- Make use of the certificates to carry out their professional activity.
- Benefit from any research and promotion activities carried out by the certification body for certified individuals.
- Claim and appeal any unfavourable decision.

6.8.2. Obligations.

Certificate holders must:

- Respect the DPO Certification Scheme and all applicable procedures.
- Comply with the financial obligations arising from certification.
- Accept the provisions of the Code of Ethics.
- Act with due technical competence in their professional sphere, ensuring they maintain the prestige of the certification granted.
- Collaborate with the certification body in the supervisory actions necessary to maintain and renew the certification.
- Inform the certification body of any professional situation that may affect the scope of the certification awarded.
- Immediately inform the certification body of any issues that may affect their ability to continue meeting certification requirements.

- Not use the certificate and the Scheme mark for uses other than those related to activities within the scope of the certification granted.
- Not carry out harmful actions of any nature, nor damage the image and/or interests of the individuals, companies, entities and clients, including potential clients, interested in professional services, nor that of the AEPD or the certification bodies.
- Not take part in fraudulent practices related to the theft and/or dissemination of exam material.
- Maintain a register of claims received related to the scope of the certification obtained.
- Return the certificate if certification is withdrawn.

Failure to comply with these obligations may result in the initiation of certificate suspension or withdrawal proceedings.

6.9. INFORMATION ON CERTIFIED PERSONS.

Certification Bodies will maintain a public registry of the status of certified persons that must be updated at least twice a year. This list will include at least their names and surnames, certificate number, date issued, expiry date, and certificate status (awarded, suspended, withdrawn, renewed) and will be available for any interested party.

7. MANAGEMENT OF COMPLAINTS AND CLAIMS REGARDING THE SCHEME

7.1. SCOPE OF APPLICATION.

Any actions contrary to the Scheme carried out by Agents or certified persons under the Scheme may be subject to compliant or claim. Behaviour by certified Data Protection Officers that violates the Scheme Code of Ethics will be of special concern.

7.2. COMPETENT BODIES.

The bodies authorised to recognise and, as applicable, resolve complaints or claims regarding the Scheme are, in this order:

- Certification Bodies (CB).
- The National Accreditation Agency (ENAC).
- Spanish Data Protection Agency (AEPD).

Any complaint or claim regarding the actions of one of the Scheme's Agents must be first filed with the corresponding Agent who made the public statement that resulted in the claim, before directing the complaint or claim to the AEPD.

Any complaint or claim by a third party, whether to the AEPD, ENAC, or an authorised CB, regarding the action or performance of an person certified under the Scheme, must be forwarded to all other agents and managed first by the authorised CB that certified the person. The responsibilities of each body will depend on the content of said complaint.

If the claim is regarding a certified person or the actions of the CB, said complaint or claim must be managed by the CB in accordance with the requirements of standard UNE-EN ISO/IEC 17024. The handling of the claims, as well as their resolution, must be verified by ENAC as part of its assessment.

If the claim is related to accreditation, it must be managed by ENAC, which must also handle claims or complaints resulting from claimants who are not satisfied by the response provided in first instance by an authorised (and therefore accredited) CB.

The AEPD may only intervene in the management and processing of any claim or complaint received regarding the operation of the Scheme when it has already been handled by the above agencies.

Any claim regarding the Scheme that is directed to the AEPD must be formally communicated to the body in writing, stating that it is a claim or complaint and that the lower body (CB or ENAC) has already attempted to resolve it. The AEPD will make a decision once the Scheme Committee has reviewed the case. The AEPD will notify the claimant of the decision made.

7.3. COMPLAINTS AND CLAIMS PROCEDURE.

The process for handling and resolving complaints or claims will be that established by the corresponding Certification Body in accordance with standard UNE-EN ISO/IEC 17024, and must be available to the public.

The procedure for managing complaints or claims regarding the Scheme must follow at least these steps:

a) Study and assessment of the complaint or appeal and, if applicable, a request for evidence.

b) Notify the interested parties and/or those affected by each appeal and claim process of the situation, and provide them with a maximum period of 30 days to present their allegations.
c) Analysis and assessment of the evidence provided and the allegations presented by the interested parties.
d) Deliberation and final decision on the matter.
e) Notification of the decision to the parties.

In order for this process to be carried out in a suitable manner, the certified individual must:

a) Fully collaborate with any open formal investigation to resolve specific cases of complaints and/or claims.

b) Maintain a registry of all of the claims filed against them related to the activities carried out in the scope of the validity of the certification and provide the Certification Body with access to these registries. For these purposes, within 10 days of receipt of a claim, they must send written notification and a copy of the claim to the Certification Body.

c) Provide clients with a form to fill out in the event of any complaint related to the services provided, which will be sent both to the certified person and to the Organisation affected by the compliant, such as the Certification Body.

If the complaint or claim merits the opening of an investigation into a certified person which could result in the temporary suspension, withdrawal or loss of certification, the provisions of section 6.7 of this Scheme shall be followed.

8. MONITORING AND SUPERVISION OF THE SCHEME

A efectos de garantizar los necesarios estándares de calidad y rigor en el cumplimiento del Esquema por los correspondientes Agentes, se constituye un Comité de Seguimiento integrado por miembros de la Agencia Española de Protección de Datos y de la Entidad Nacional de Acreditación para realizar el seguimiento y control del funcionamiento del mismo, especialmente durante las primeras etapas de su aplicación.

ANNEXES

Annex I. Conditions for demonstrating compliance with pre-requisites.

Annex II. Mark of the Scheme.

- Annex II.A. Rules of use for the Mark of the Scheme.
- Annex II.B. Template for the concession of use contract for the Mark of the Scheme between the AEPD and Scheme's Agents.

Annex III. Code of Ethics .

Annex IV. Exam Programme (topics).

Annex V. Procedure for selecting and appointing evaluators.

Annex VI. Template for proof of certification document.

ANNEX I
CONDITIONS FOR DEMONSTRATING COMPLIANCE WITH PRE-REQUISITES

A. TRAINING.

- Provide a certificate of having received minimum recognised training on subjects related to the Scheme programme.
- Depending on pre-requisites, demonstrate training of 60, 100 or 180 hours.
- The recognition of training programmes will be made by the Certification Entities according to the requirements defined in the Scheme.
- The distribution of the hours of the training programmes will follow the same percentage established for each one of the domains of the program of the Scheme. A training programme may consist of several courses.
- The distribution for training of 60 hours will be as follows:
    - Domain 1 - 30 hours, Domain 2 - 18 hours, Domain 3 - 12 hours
- The distribution for training of 100 hours will be as follows:
    - Domain 1 - 50 hours, Domain 2 - 30 hours, Domain 3 - 20 hours
- The distribution for the training of 180 hours will be as follows:
    - Domain 1 - 90 hours, Domain 2 - 54 hours, Domain 3 - 36 hours
- For training expressed in ECTS[1] or LRU[2] credits (referred to university education, including internships or graduation projects), 1 ECTS is considered to be 25 hours and 1 LRU is 10 hours.

B. WORK OR PROFESSIONAL EXPERIENCE.

Demonstrate the work or professional experience required by the pre-requisites: two, three or five years of experience. To do so, candidates must submit objective proof of general and specific experience through a statement from their employer or client, work contract, etc.

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

Experience processing high-risk personal data will be counted as twice the time as years of experience processing non-high risk personal data.

If a certain work experience did not last a full year, experience equal to or greater than six months will be counted as half of a year.

If a candidate does not have the experience required, up to one year of experience, i.e. 60 points, may be recognised by demonstrating additional qualifications.

Teaching training will also be considered as work experience and, in particular, it will be assessed as twice the hours as receiving training.

For training taught on a specific topic, only one of the editions taught will be accepted if there are more than one with the same title and curriculum.

The scale in table 1 will be used to calculate experience.

Table 1

Training	Experience	Points for one year of experience	Minimum required experience points
-	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. RECOGNITION OF ADDITIONAL QUALIFICATIONS.

If candidates reach the number of points required through the professional experience pre-requisites, it will not be necessary to assess any additional qualifications. The following table of qualifications will only be used to complete scoring if a candidate does not meet the minimum number of points required due to a lack of years of experience.

Aspects already considered as pre-requisites will not be assessed as qualifications.

The scale in table 2 will be used to calculate additional qualifications.

Table 2

Category	Maximum Points	Qualification	Unit Points[3]	Max.
Specific or complementary university education on data protection or privacy, according to EHEA.[4]	30	Bachelor's degree or technical engineering degree	6	12
		Unofficial postgraduate or master's degree	6	12
		Official postgraduate degree	8	16
		Official master's degree	10	20
		Doctorate	9	9
Specific or complimentary training on data protection or privacy.	50	Attending courses, seminars, events, sessions or conferences organised or expressly recognised by Data Protection Certification Authorities or Bodies (minimum 1 credit or 10 hours)	1	25
		Attending non-university courses or seminars organised by professional organisations (minimum 2 credits or 20 hours)	0.20	10
		Attending university courses or seminars (minimum 2 credits or 20 hours)	0.50	10
		Attending events, sessions or conferences on the specialisation, which must total at least 20 hours per year.	0.50	5
Graduation project on data protection or privacy.	5	Pass the graduation project and spend at least 40 hours on it.	1.5	5
Internships at companies on data protection or privacy.	5	At least 40 hours of internship at a company.	1.5	5
Work experience in data protection or privacy.	50[5]	Specific privacy functions at the job, per year of experience	10	30
		Professional or employee carrying out different activities, per project (complexity, duration and role played will be considered)	5	20
Teaching activity related to data protection or privacy.	30	Teaching at university degree programmes (per every 10 hours)	0.5	10
		Professor for basic level courses/seminars (per every 20 hours) Professor for specialised courses and seminars (per every 10 hours)	0.2	5
		Teacher of Training Entity courses (per every 10 hours)	0.5	10

[3] Attributable to each qualification considered individually. In specific cases such as attending events, a unit will have been reached when the total number of minimum recognised hours has been accredited.
[4] According to EHEA: European Higher Education Area.
[5] Experience other than that used as a pre-requisite.

		Speaker or presenter at conferences (per event)	0.1	5
Research activity and publications on data protection or privacy topics.	20	Authorship or co-authorship of books	2.5	8
		Authorship or co-authorship of book chapters, conference reports, and similar documents.	0.5	5
		Authorship or co-authorship of articles in specialised journals and publications.	0.25	5
		Authorship or co-authorship of contributions in the media or blogs.	0.10	2
Data protection or privacy awards.	10	Awards and professional or similar recognitions.	5	10
Data protection and privacy certifications (current).	10	ACP-DPO from APEP, CDPP from ISMS FORUM[6], ECPC-B DPO from Maastricht University, DPO from EIPA (European Institute of Public Administration), or similar certification.	4	10
Other certifications on related topics (current).	10	ACP-B/ACP-CL/ACP-CT/ACP-AL/ACP-AT from APEP, CDPP from ISMS FORUM[7], CISA/CISM/CRISC from ISACA, CISSP from Certified Information Systems Security Professional (ISC)[2], CIPP/CIPT from IAPP (International Association of Privacy Professionals), Auditor ISO 27001 or similar certification.	2	10

[6] New CDPP from December 2016.
[7] Former CDPP prior to December 2016.

ANNEX II.A
RULES OF USE FOR THE MARK OF THE SCHEME

1. MARK OF THE SCHEME.

The AEPD-DPO Mark of the Scheme has been created so that the market can identify persons certified as "Data Protection Officers" (DPO) promoted by the AEPD.

The Mark of the Scheme is the symbol used by certification scheme Agents to make this fact known publicly.

The Mark of the Scheme will be used exclusively by the AEPD, authorised certification bodies, ENAC and authorised training agencies/academies.

The design and characteristics of the Mark of the Scheme are specified in the Annex of this document.

2. USES.

The Mark of the Scheme will be used exclusively to indicate that the agent in question is authorised by the AEPD as an agent involved in implementing the scheme.

It may not be used by persons, regardless of whether they are certified as DPO in accordance with the scheme's rules.

Nor may it be used by any agent during their provisional authorisation period, and not until they have obtained the corresponding accreditation from ENAC.

3. RULES OF USE.

The conditions of use for the Mark of the Schemeare as follows:

a) It may only be used by agents after they are expressly authorised by AEPD to do so in relation with the "Data Protection Officer" certification.

b) It will always be clearly associated with the name or logo of the authorised agent.

c) The agent may use it on advertising documents or media (brochures, websites, etc.) in such a way that its connection solely to the AEPD "Data Protection Officer" certification service is clear, and that does not imply a connection with any other similar service that is offered on the market.

d) Any use of the Mark of the Scheme (for example, on business cards) is not authorised for authorised agent employees or collaborators, including those who work for AEPD or members of the Scheme Committee.

e) The agent must cease to use the Mark of the Scheme if their authorisation is suspended during the period of the suspension, and must do so permanently if they lose authorised agent status, whether due to a voluntary withdrawal, loss of ENAC accreditation (in the case of certification bodies), or for any other reason.

ANNEX

Mark to be determined by the Agency at a later date.

ANNEX II.B
TEMPLATE FOR THE CONCESSION OF USE CONTRACT FOR THE MARK OF THE SCHEME BETWEEN THE AEPD AND SCHEME'S AGENTS

CLAUSE ONE. MARK OF THE SCHEME.

The Mark of the Scheme has been created so that the market can identify individuals certified as "Data Protection Officers" (DPO) promoted by the AEPD Scheme; the Mark will be the symbol used by AEPD-DPO Certification Scheme Agents to make this fact known publicly.

This mark will be used exclusively by the AEPD, authorised Certification Bodies, ENAC, and, as appropriate, authorised Training Entities.

The design and characteristics of the Mechanism Seal are those established in the Annex "Rules of Use for the AEPD-DPO Mechanism Seal".

CLAUSE TWO. USES.

The Mark of the Schemewill be used exclusively to indicate that the agent in question is authorised by the AEPD as an agent involved in implementing the Scheme.

It may not be used by natural persons, regardless of whether they are certified as a DPO in accordance with the Scheme's rules.

It may not be used by any agent during their provisional authorisation period, and not until they have obtained the corresponding accreditation from ENAC.

CLAUSE THREE. RULES OF USE.

Use of the Mark of the Scheme will be subject to the following rules:

a) It may only be used by agents after they are expressly authorised by AEPD to do so in relation with the "Data Protection Officer" certification.

b) It will always be clearly associated with the name or logo of the authorised agent.

c) The Agent may use the Mark of the Scheme on advertising documents or media (brochures, websites, etc.) in such a way that its connection solely to the AEPD "Data

Protection Officer" certification service is clear, and that does not imply a connection with any other similar service that is offered on the market.

d) The Agent must cease to use the Mark of the Scheme if their authorisation is suspended during the period of the suspension, and must do so permanently if they lose authorised agent status, whether due to a voluntary withdrawal, loss of ENAC accreditation (in the case of certification bodies), or for any other reason.

e) Any use of the Mark of the Scheme (for example, on business cards) is not authorised for authorised Agent employees or collaborators, including those who work for AEPD or members of the Scheme Committee.

ANNEX III
CODE OF ETHICS FOR PERSONS CERTIFIED AS DATA PROTECTION OFFICERS IN ACCORDANCE WITH THE SPANISH DATA PROTECTION AGENCY SCHEME

PREAMBLE

This Code is an express statement of the values, principles, and rules that must guide the conduct of persons certified as Data Protection Officers (DPO) in accordance with the Spanish Data Protection Agency (AEPD) Certification Scheme in the exercise of their functions or tasks, and in their relations with other employees, as well as with clients, providers, public and private institutions, external collaborators and society in general.

The Code of Ethics, therefore, groups together the commitments regarding integrity, impartiality, legality, confidentiality, and transparency that those who aim to be Data Protection Officers certified under the AEPD Scheme must invariably follow, understand, and disseminate.

Thus, with this Code we aim to prevent behaviour contrary to the criteria contained herein, while designing monitoring and control mechanisms that guarantee full compliance herewith by all persons who work professionally as DPO certified by the AEPD Scheme.

The criteria for conduct contained in this Code do not intend to cover all situations or circumstances that the aforementioned professionals may confront, but rather to establish general guidelines of conduct that can guide their actions as they go about their professional activity.

ARTICLE I. SCOPE OF APPLICATION.

The principles, values and criteria contained in this Code of Ethics must be followed by the Data Protection Officers certified by the certification bodies accredited by the National Accreditation Agency (ENAC) under the AEPD Scheme.

ARTICLE II. GENERAL PRINCIPLES.

DPOs certified in their professional activity according to the AEPD Scheme must carry out their activity in compliance with the following principles:

- **Legality and integrity**, strictly complying with current legislation, in particular regarding the service they provide, so as to avoid performing any illicit activity.

- **Professionalism**, performing their functions with due diligence and professional rigour, and maintaining their professional capacity and personal training constantly up to date; they must behave before individuals, companies, entities and clients in a scrupulously loyal manner and regardless of any type of limitations that may influence their own work and that of the personnel they may be responsible for.

- **Responsibility** in carrying out their professional and personal activity, undertaking only those activities that they can reasonably expect to complete with the necessary skills, knowledge and competence.

- **Impartiality**, acting objectively without accepting the influence of conflicts of interest or other circumstances that could question their professional integrity and that of the organisation to which they belong;

- **Transparency**, informing all interested parties in a clear, precise, and sufficient manner of all aspects related to their professional activity, provided said aspects are not subject to confidentiality, in which case they will be reserved and may not be divulged;

- **Confidentiality**, respecting and maintaining the necessary protection and discretion regarding the information to which they may have access because of their professional activity, safeguarding the right to privacy of all interested parties. Such information may not be used for personal benefit nor revealed to inappropriate parties.

ARTICLE III. RELATIONS WITH ORGANISATION PERSONNEL.

In their relations with other employees, managers, and collaborators with the organisation, Data Protection Officers:

- Must interact fairly and respectfully with other employees or managers at their organisation.

- Will assume responsibility for their actions and those of their collaborators, promoting their professional development through motivation, training and communication. In all cases, the relationship with collaborators must be based on mutual respect and quality in management.

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

- They will ensure that the personnel under their responsibility do not carry out any illicit activity or behaviour contrary to this code of ethics.

- They will always provide all of the information needed to adequately monitor their activity, without hiding errors or non-compliance, and aiming to correct any deficiencies detected.

ARTICLE IV. RELATIONS WITH EXTERNAL COLLABORATORS AND PROVIDERS.

In their relations with external collaborators and providers, Data Protection Officers:

- Will establish relationships based on trust, respect, transparency and mutual benefit.

- Will act impartially and objectively in selection processes for these personnel, applying criteria of competence, quality and cost, avoiding conflicts of interests at all times. Hiring of services or procurement of goods must be carried out with fully independent decision-making and outside of any personal, family or economic connection, which could call into question the criteria used in the selection.

ARTICLE V. RELATIONS WITH CLIENTS.

In their relations with clients, Data Protection Officers:

- Will disclose the content of this Code of Ethics.

- Will act in a trustworthy, professional fashion, aiming to achieve a high level of quality in their services and to develop long-term relationships based on trust and mutual respect.

- Will always safeguard their independence, preventing their professional activity from being influenced by economic or family ties or friendship with clients, or with their professional relations outside of their work as DPO. They may not accept fees, gifts, or favours of any type from clients or their representatives.

- Will not make or accept, directly or indirectly, any payment or service of greater value other than that freely agreed to with their employer.

- Will report to their client any conflict of interest that may exist in their professional relationship regarding the certification before accepting a professional assignment.

- Will not perform any promotional activity (advertising, informational material or other) that may lead clients to an incorrect interpretation of the meaning of the certifications under the AEPD Scheme, or to unrealistic expectations.

- Will provide clients with a form to fill out in the event of any complaint related to the services provided, which will be sent both to the certified person or to the Organisation affected by the complaint, and to the Certification Body.

ARTICLE VI. COLLABORATION WITH CERTIFICATION BODIES.

DPOs will fully collaborate with any formal investigation regarding violations of this code initiated by the Certification Bodies or to resolve specific complaints and/or claims.

For this purpose, they must maintain a registry of all of the claims filed against them related to the activities carried out in the scope of the validity of the certification and provide the Certification Body with access to these registries. Within 10 days of receipt of a claim, they must send written notification and a copy of the claim to the Certification Body.

ARTICLE VII. RELATION WITH AUTHORITIES AND PUBLIC ADMINISTRATIONS.

Relations with institutions, bodies and national, regional and local public administrations, especially with the Supervisory Authority, will be carried out following standards of utmost collaboration and scrupulous compliance with their decisions. Notifications, summons, and requests for information must be attended with diligence, within established deadlines.

ARTICLE VIII. PERFORMANCE OF OTHER PROFESSIONAL ACTIVITIES.

DPOs will not carry out activities that directly or indirectly compete with the AEPD and/or Certification Body.

To that end, they will communicate to their organisation the performance of any other work, professional, or business activity (paid or unpaid) that takes place within or outside of working hours, or their significant participation as partners in private companies or businesses, so that it may be assessed whether this activity is compatible with their work or with the purposes or objectives of the organisation.

ARTICLE IX. ACCEPTANCE AND INTERPRETATION OF THE CODE OF ETHICS.

The subjects included in the scope of application of this Code are responsible for understanding and complying with it, and therefore must understand its content and have signed it. The AEPD Scheme requires a high level of commitment from DPOs in complying with this Code of Ethics.

Any questions they may have about the interpretation or application of this document must be directed to the Certification Body, which is required to promote knowledge of and compliance with the Code and interpret it in the event of any questions.

ARTICLE X. FAILURE TO COMPLY WITH THE CODE OF ETHICS.

Failure to comply with any of the principles, values and criteria set out in this Code may result in an investigation into the conduct of the holder of the certification and, ultimately, in disciplinary measures from the corresponding certification body, which could mean suspension or removal of the certification.

ANNEX IV. EXAM PROGRAMME (TOPICS).

SCHEME PROGRAMME/SYLLABUS
CONTENTS

1. Field 1. GENERAL DATA PROTECTION REGULATIONS.

(percentage of syllabus: 50%)

1.1. Regulatory context.

1.1.1. Privacy and data protection in the international sphere.
1.1.2. Data protection in Europe.
1.1.3. Data protection in Spain.
1.1.4. Standards and best practices.

1.2. European Data Protection Regulation and update of the LOPD. Foundations.

1.2.1. Scope of application.
1.2.2. Definitions.
1.2.3. Entities bound by the regulation.

1.3. European Data Protection Regulation and update of the LOPD. Principles

1.3.1. The right/responsibility binomial in data protection.
1.3.2. Lawfulness of processing
1.3.3. Loyalty and transparency
1.3.4. Limitation of the purpose
1.3.5. Minimisation of data
1.3.6. Accuracy

1.4. European Data Protection Regulation and update of the LOPD. Legitimation

1.4.1. Consent: granting and revocation.
1.4.2. Informed consent: purpose, transparency, storage, information and data subject's notification responsibility.
1.4.3. Consent of children.
1.4.4. Special data categories.
1.4.5. Data regarding criminal offences and convictions.
1.4.6. Processing which does not require identification.
1.4.7. Legal bases other than consent.

1.5. Rights of individuals.

1.5.1. Transparency and information
1.5.2. Access, rectification, erasure (right to be forgotten).

1.5.3. Right to object
1.5.4. Automated individual decision-making.
1.5.5. Portability.
1.5.6. Restriction of processing.
1.5.7. Restrictions on rights.

1.6. European Data Protection Regulation and update of the LOPD. Compliance measures.

1.6.1. Data protection policies.
1.6.2. Legal status of participants. Controllers, co-controllers, processors, sub-processors and their representatives. Relationships and formalisation.
1.6.3. Record of processing activities: identification and classification of data processing.

1.7. European Data Protection Regulation and update of the LOPD. Accountability.

1.7.1. Privacy by design and by default. Fundamental principles.
1.7.2. Impact assessment regarding data protection and prior consultation. High-risk processing.
1.7.3. Personal data security. Technical and organisational security.
1.7.4. Security breaches. Reporting security breaches.
1.7.5. Data Protection Officer (DPO). Regulatory framework.
1.7.6. Codes of conduct and certifications.

1.8. European Data Protection Regulation. Data Protection Officers (DPO).

1.8.1. Designation. Decision-making process. Appointment, renewal and removal processes. Analysis of conflict of interests.
1.8.2. Obligations and responsibilities. Independence. Identification and reporting to management.
1.8.3. Procedures. Collaboration, previous authorisations, relations with data subjects and complaint management.
1.8.4. Communication with 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. European Data Protection Regulation and update of the LOPD. International data transfers

1.9.1. Adecuacy decisions system.
1.9.2. Transfers subject to appropriate safeguards.
1.9.3. Binding Corporate Rules
1.9.4. Exceptions.
1.9.5. Authorisation of the supervisory authority.

1.9.6. Temporary suspension
1.9.7. Contract clauses

1.10. European Data Protection Regulation and update of the LOPD. Supervisory Authorities.

1.10.1. Supervisory Authorities.
1.10.2. Powers.
1.10.3. Penalty system.
1.10.4. European Data Protection Board.
1.10.5. Procedures followed by the AEPD.
1.10.6. Jurisdictional protection.
1.10.7. Right to compensation.

1.11. RGPD interpretation guidelines.

1.11.1. Guides from the Art. 29 WG.
1.11.2. Opinions of the European Data Protection Board
1.11.3. Standards of judicial bodies.

1.12. Sectoral regulations affected by data protection.

1.12.1. Health, pharmaceutical, research.
1.12.2. Protection of children
1.12.3. Financial 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 11 July on Information Society Services and E-Commerce
1.13.2. LGT, Law 9/2014 of 9 May, General Telecommunications Act
1.13.3. E-signature law, Law 59/2003, of 19 December, on e-signatures

1.14. European regulations with data protection implications.

1.14.1. ePrivacy Directive: Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) or ePrivacy Regulation when approved.
1.14.2. Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009, amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic

communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws.

1.14.3. Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

2. Field 2. ACCOUNTABILITY.

(percentage of syllabus: 30%)

2.1. Analysis and management of personal data processing risks.

2.1.1. Introduction. General framework of risk assessment and management. General concepts.
2.1.2. Risk assessment. 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. Assessment of protection. Residual risk, acceptable risk and unacceptable risk.

2.2. Risk analysis and management methodologies.

2.3. Data Protection and Security compliance programme at an organisation.

2.3.1. Designing and implementing a data protection programme in the context of the organisation.
2.3.2. Objectives of the compliance programme.
2.3.3. Accountability: Traceability of the compliance model.

2.4. Information security.

2.4.1. Regulatory framework. National Security Scheme and NIS directive: Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union. Scope of application, objectives, main elements, basic principles and minimum requirements.
2.4.2. Cybersecurity and information security governance. General notions, mission, effective governance of Information Security (IS). IS Concepts. Scope. Metrics of IS governance. State of IS. IS strategy.
2.4.3. Implementation of information security. Security by design and by default. The life cycle of Information Systems. Integrating security and privacy into the life cycle. IS quality control.

2.5. Data Protection Impact Assessment “DPIA”.

2.5.1. Introduction and basics of DPIA: Origin, concept, and characteristics of DPIA. Scope and need. Standards.
2.5.2. Performing an impact assessment. Preparatory and organisational aspects, analysis of the need to carry out an assessment and prior consultations.

3. Field 3. TECHNIQUES TO ENSURE COMPLIANCE WITH DATA PROTECTION REGULATIONS.

(percentage of syllabus: 20%)

3.1. Data protection audits.

3.1.1. The audit process. General matters and introduction to auditing. Basic characteristics of the Audit.
3.1.2. Drafting the audit report. Basic aspects and importance of the audit report.
3.1.3. Execution and monitoring of corrective actions.

3.2. Information Systems Audit.

3.2.1. The role of Information System Audits. Basic concepts. Standards and guidelines for IS audits.
3.2.2. Internal control and continuous improvement. Best practices. Integrating the data protection audit into the IS audit.
3.2.3. Planning, execution and monitoring.

3.3. Security of processing management.

3.3.1. National Security Scheme, ISO/IEC 27001:2013 (UNE ISO/IEC 27001:2014: Requirements for Information Security Management Systems, ISMS).
3.3.2. Security of Assets Management. Security in software and procedures. Security applied to information technologies and documentation.
3.3.3. Recovering from disasters and business continuity. Protecting technical and document assets. Planning and management of Disaster Recovery.

3.4. Other knowledge.

3.4.1. 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 most recent technologies

ANNEX V
PROCEDURE FOR SELECTING AND APPOINTING EVALUATORS

Evaluators may be personnel from the entity itself or subcontracted (self-employed or hired by the entity).

The provisions of their contract will apply to any issues that may arise regarding non-compliance with their commitments under the Scheme.

This procedure establishes the criteria regarding selection and renewal processes for subcontracted companies or individuals.

1. Records and work procedures.

The CVs of all of the evaluators will be kept on file, and will include records on qualifications, training and experience that demonstrate their suitable technical competence.

Furthermore, evaluators will be given copies of quality control system documents applicable to their work, and especially all procedures and forms that are applicable to their evaluation activity.

2. Requirements for evaluators.

Candidate evaluators must meet the following requirements.

a) Undergraduate degree.

b) At least five years of experience in data protection or information security.

3. Qualifications.

The following qualifications are desirable:

3.1. Preferred qualifications.

1. Advanced university degree: doctorate, postgraduate or master's degree in data protection or information security.
2. Teaching experience in subjects related to data protection and information security.
3. Hold certifications related to data protection or information security in the last five years.

3.2. Additional qualifications.

The following qualifications are also valued:

1. Over five years of experience in data protection or information security.
2. Participation in national or international standardisation committees related to data protection or information security.
3. Publication of articles on either subject.

4. Incompatibilities and exclusions.

Individuals whose independence may be compromised due to any professional, family, or personal circumstance may be partially or fully excluded from the evaluation process.

5. Evaluator functions.

The evaluator is responsible for:

1. Impartially and confidentially evaluating the documentation submitted by candidates and their exams. Exams will be graded without knowing the identity of the candidate.
2. Issue a report with the result of the evaluation.

Additionally, they must:

1. Inform the Certification Body of any professional, family, or other relationship that may affect the objectivity and impartiality of their evaluation work.
2. Assess the grounded recusal of any candidate to notify the Certification Body.

6. Selection procedure.

The Certification Body will assess the candidacies of evaluators and will reach a decision, notifying the candidate of such decision.

7. Selection committee.

The Certification Body will create an internal body subject to internal regulations and Scheme rules to select evaluators.

ANNEX VI
CONTENT OF THE CERTIFICATION OF COMPLIANCE WITH THE SPANISH DATA PROTECTION AGENCY'S DATA PROTECTION OFFICER SCHEME

Each Certification Body can use its own format for the Certification of Compliance with the AEPD Data Protection Officer Scheme, but it must include at least the following content:

— Logo of the Certification Body.

— Identification of the Certification Body.

— Logo of Data Protection Officer Certification Scheme.

— Text: "Certificate of Compliance with the AEPD Data Protection Officer Certification Scheme".

— Text: "[Certification Body] hereby certifies that the following candidate has been assessed and found to meet the requirements of the Spanish Data Protection Agency's Data Protection Officer Certification Scheme:"

— [identify the individual receiving certification with their name, surnames and Spanish ID].

— Text: "Certificate number: [certificate number]".

— Text: "Date of initial certification of compliance: [day] [month], [year]".

— Text: "Date of renewal of certification of compliance: [day] [month], [year]".

— Text: "Expiry date of certification of compliance: [day] [month], [year]".

— Text: "Date: [Town], [day] [month], [year]".

— Signature: Name and surnames of the competent authority from the Certification Body.

The text between brackets should be adapted to the specific aspects of the certification being issued.

Below is an example template of the aforementioned Certification of compliance.

Logo of the Certification Body with accreditation mark

LOGO OF THE DATA PROTECTION OFFICER CERTIFICATION SCHEME

Certification of Compliance with the Spanish Data Protection Agency's Data Protection Officer Scheme

The Certification Body can use its own format for the Certification of Compliance with the AEPD Data Protection Officer Scheme, but it must include at least the following content:

— Logo of the Certification Body.

— Identification of the Certification Body.

— Logo of Data Protection Officer Certification Scheme.

— Text: “Certificate of Compliance with the AEPD Data Protection Officer Certification Scheme”.

[Certification Body] hereby certifies that the following candidate

has been assessed and found to meet the requirements of the Spanish Data Protection Agency’s Data Protection Officer Certification Scheme, as indicated in the corresponding Certification Report dated [date] for:

[identify the individual receiving certification with their name, surnames and Spanish ID].

“Date of initial certification of compliance: [day] [month], [year]

“Date of renewal of certification of compliance: [day] [month], [year]”

“Certificate number: [certificate number]

“Date: [Town], [day] [month], [year]”

Signature: [Name and surnames of the competent authority from the Certification Body]

Signature of Certification Body official.

Full name/company name of the Certification Body and website.

Postal or electronic address

Post Code, Province, Country.

CERTIFICATION SCHEME OF DATA PROTECTION OFFICERS FROM THE SPANISH DATA PROTECTION AGENCY (DPO-AEPD SCHEME).

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS