Experto Delegado de Protección de Datos

de 180 horas de duración

Con la colaboración de UBT Legal & Compliance

Presentación

El Reglamento Europeo de Protección de Datos, aplicable desde el 25 de mayo de 2018, supuso un cambio sustancial en las obligaciones de las organizaciones relacionadas con la Protección de Datos, exigiendo garantizar y acreditar su cumplimiento mediante una gestión responsable.

El Reglamento introdujo la figura del Delegado de Protección de Datos que asume la supervisión y coordinación de su cumplimiento. Figura que debe ser designada atendiendo a sus cualidades profesionales, conocimientos teóricos y prácticos y su capacidad para desempeñar las funciones indicadas en el Reglamento.

Esta figura es de obligado cumplimiento en:

- Autoridades y organismos públicos
- Empresas que traten datos sensibles a gran escala
- Empresas que realicen seguimiento de personas de forma sistemática y a gran escala
- Aseguradoras, entidades financieras y de inversión, centros docentes, prestadores de servicios de la sociedad de la información, ….

Esta posición del DPD es fundamental para gestionar y garantizar en las organizaciones el cumplimiento de la normativa, tanto si está obligada como no a disponer de esta figura. Nuestra formación será clave del éxito de la competencia y ejercicio eficaz de esta función.

La Agencia Española de Protección de Datos (AEPD) ha impulsado el desarrollo de un modelo de certificación como Delegado de Protección de Datos, con el objetivo de ofrecer seguridad y fiabilidad tanto a los profesionales de la privacidad como a las empresas y entidades que van a incorporar esta figura a sus organizaciones o que necesitan contratar los servicios de un profesional cualificado.

Objetivo general:

Proporcionar una formación en la normativa relacionada con la Protección de Datos Personales, así como en las técnicas y conocimientos para una aplicación efectiva de la misma, de 180 horas de duración, dirigida a profesionales con menos de 2 años de experiencia en proyectos y/o actividades y tareas relacionadas con las funciones del Delegado de Protección de Datos (DPD).

Objetivos específicos:

- Obtener una visión general de la normativa europea de Protección de Datos, resaltando los aspectos prácticos que afectan a las entidades responsables de los tratamientos y a sus prestadores de servicios.
- Conocer los principios básicos del Reglamento Europeo de Protección de Datos.

- Analizar en detalle las obligaciones que afectan a aquellas entidades públicas y privadas que tratan datos de carácter personal.
- Comprender la metodología de la gestión responsable conforme al principio de Accountability. Gobernanza y garantía de cumplimiento.
- Conocer los derechos que afectan a los interesados y la forma de atenderlos. Estatuto del DPD.
- Conocer el nuevo régimen sancionador, así como las funciones que asumen las autoridades nacionales y las instituciones comunitarias en el control del cumplimiento de la normativa de Protección de Datos.
- Exponer las nuevas obligaciones de seguridad, la forma de identificar los riesgos y aplicar las medidas destinadas a paliar o mitigar los mismos y las metodologías para su implantación y revisión periódica.
- Analizar las funciones del Delegado de Protección de Datos (DPO), obteniendo los conocimientos de la normativa requeridos para poder llevarlas a cabo.
- Conocer la forma de cumplir las obligaciones del Reglamento Europeo de Protección de Datos.
- Capacitarse para detectar los riesgos de incumplimiento de la norma, implementar correctamente las medidas necesarias y verificar eficazmente la aplicación de las mismas.
- Conocer las especificaciones y obligaciones en materia de seguridad en la utilización de medios electrónicos en el ámbito de las competencias de las Administraciones Públicas. Esquema Nacional de Seguridad.
- Conocer los delitos que se pueden cometer a través de redes de comunicación electrónicas, tales como el hacking, phishing, cracking, sexting o DoS, así como su tipificación actual en el Código Penal y la forma de prevenirlos, haciendo hincapié en aquellos que pueden afectar a datos de carácter personal.
- Entender los fundamentos y conceptos de los Sistemas de Gestión de Seguridad de la Información (SGSI)
- Conocer los estándares internacionales ISO 27001 e ISO 27002, los requisitos para la implantación y la auditoría del SGSI.
- Conocer la normativa sectorial que regula o afecta al tratamiento de datos de carácter personal en el ámbito público, en el ámbito privado, sanitario y en entornos informáticos.
- Analizar la normativa que regula la grabación de imágenes.
- Identificar los retos jurídicos basados en la aplicación de las nuevas tecnologías.
- Aplicar los conocimientos adquiridos realizando ejercicios y casos prácticos diseñados a tal efecto.
- Prepararse para superar el examen de certificación oficial como Delegado de Protección de Datos (siempre que cumpla con los requisitos de experiencia o formación necesarios para presentarse al mismo).

PROGRAMA DPO-C

Contenido:

- **Sesiones 1 a 4**

  Normativa general de protección de datos, responsabilidad proactiva y técnicas para garantizar el cumplimiento.

  Presencial: 28 h en 4 sesiones de 7 horas.

  Online: 28 horas

- **Sesión 5 y 6**

  Responsabilidad activa, gestión riesgos y seguridad información

  Presencial: 14 h en 2 sesiones de 7 horas.

  Online: 4 horas

- **Sesión 7**

  Técnicas para garantizar el cumplimiento de la normativa de protección de datos

  Presencial: 7 h en 1 sesiones.

  Online: 2 horas

- **Sesión 8**

  Normativa general de protección de datos. Registro de tratamiento y seguridad

  Presencial: 7 h en 1 sesiones.

  Online: 11 horas

- **Sesión 9**

  Análisis de riesgos y evaluación de impacto

  Presencial: 7 h en 1 sesiones.

  Online: 12 horas

- **Sesión 10**

  Normativas sectoriales, española y europea. Implicación de la tecnología

  Presencial: 7 h en 1 sesiones.

  Online: 4 horas

- **Sesión 11**

  Técnicas para garantizar el cumplimiento. Fundamentos ISO 27002 y SG de seguridad de la información ISO 27001

  Online: 8 horas

- **Proyecto**

  Online: 37 horas

- **Repaso y evaluación final**

  Online: 4 horas

Modalidad

Semipresencial

Sesiones presenciales: 70 horas presenciales en 10 sesiones de 7 horas.

Sesiones online: 110 horas distribuidas a lo largo de las diferentes sesiones y basadas en el estudio de contenidos teóricos, lecturas relacionadas, realización de test, participación en foros de debate, desarrollo de actividades prácticas individuales o grupales, realización de proyecto y evaluación final.

URL: campusonline.aenor.com

El contenido se ajusta a los dominios recogidos en el Esquema de Certificación de la Agencia Española de Protección de Datos:

- Dominio 1: 90 horas
- Dominio 2: 54 horas
- Dominio 3: 36 horas

Criterios de superación del programa:

- Participación en las sesiones
- Realización de casos y ejercicios prácticos
- Participación en foros y debates
- Realización de examen
- Entrega de proyecto final

Profesores

Óscar López Rodríguez-Director técnico del programa Experto Delegado de Protección de Datos de 180 horas de duración

Director General de UBT Compliance Services,S.L, abogado con más de 15 años de experiencia especializado en privacidad, derecho de las tecnologías de la información e internet, evidencias electrónicas y Corporate Compliance.

Auditor experto y profesor, desde el año 2003, en AENOR en distintas normas como ISO/IEC 27001, UNE 71505, ISO 27037, UNE 19600, UNE 19601 e ISO 37001. Docente en el Instituto de Estudios Bursátiles y en el Ilustre Colegio de Abogados de Madrid, colaborador de ISACA, miembro del Instituto para el Cumplimiento Normativo y la Prevención del Fraude y de la Asociación Nacional de Compliance.

Imparte materia de los epígrafes: 1.1, 1.2, 1.3, 1.4, 1.4, 1.6, 1.7, 1.8, 1.9, 1.10, 1.10, 1.11, 1.12, 1.13, 1.14, 2.1, 2.2, 2.3, 2.4, 2.5, 3.1, 3.2, 3.3, 3.4

Fernando Cuadrado Malasaña

Abogado en ejercicio desde el año 1992 y Delegado de Protección de Datos, con más de cinco años de experiencia impartiendo clases sobre protección de datos, privacidad y seguridad de la información.

Profesor en el máster en blockchain aplicado de la Universidad Europea Miguel de Cervantes y en el máster Universitario en Derecho de la Ciberseguridad y entorno digital de la Universidad de León; profesor de seguridad acreditado por el Ministerio del Interior.

Imparte materia de los epígrafes: 1.1, 1.2, 1.3, 1.4, 1.4, 1.6, 1.7, 1.8, 1.9, 1.10, 1.10, 1.11, 1.12, 1.13, 1.14, 2.1, 2.2, 2.3, 2.4, 2.5, 3.1, 3.2, 3.3, 3.4

Santiago Cruz Roldán

Abogado especializado en protección de datos, contratación tecnológica y propiedad intelectual. Consultor de privacidad. Implantación de protocolos LOPD – RGPD. Asesoramiento en materia de protección de datos y ciberseguridad.

Cuenta con más de cinco años de experiencia impartiendo formaciones en materia de ciberseguridad, privacidad y protección de datos.

Imparte materia de los epígrafes: 1.1, 1.2, 1.3, 1.4, 1.4, 1.6, 1.7, 1.8, 1.9, 1.10, 1.10, 1.11, 1.12, 1.13, 1.14, 2.1, 2.2, 2.3, 2.4, 2.5, 3.1, 3.2, 3.3, 3.4

Juan Miguel Pulpillo Fernández

Abogado auditor certificado en entornos tecnológicos, DPO, Compliance Officer, analista de Ciberinteligencia y Ciberseguridad, instructor de la Directiva (UE) 2019/1937 y de Compliance. Credencial Profesional Nivel Negro en Ciberseguridad Industrial.

Profesor de máster y cursos de experto en materias como Internet, Privacidad, IT, Audiovisual, Marketing Digital, Telecomunicaciones, Seguridad, Cloud Computing, Big Data, IoT,… en diversas universidades e instituciones.

Imparte materia de los epígrafes: 1.1, 1.2, 1.3, 1.4, 1.4, 1.6, 1.7, 1.8, 1.9, 1.10, 1.10, 1.11, 1.12, 1.13, 1.14, 2.1, 2.2, 2.3, 2.4, 2.5, 3.1, 3.2, 3.3, 3.4

Jesús Soler Puebla

Abogado, socio de Privacidad Digital Abogados, vinculado desde el inicio de su carrera al mundo de la Protección de Datos. Fundador de Olvídame.es, especialistas en Derecho al Olvido y Defensa Jurídica de la Reputación OnLine. Miembro fundador del Registro de Auditores Jurídicos en entornos tecnológicos del Colegio de Abogados de Barcelona.

Es miembro del comité científico y profesor del Máster en Derecho de la Sociedad de la Información.

Imparte materia de los epígrafes: 1.1, 1.2, 1.3, 1.4, 1.4, 1.6, 1.7, 1.8, 1.9, 1.10, 1.10, 1.11, 1.12, 1.13, 1.14, 2.1, 2.2, 2.3, 2.4, 2.5, 3.1, 3.2, 3.3, 3.4

Tristan Ramaget

Ingeniero superior de telecomunicaciones, consultor experto y auditor en SGSI ISO 27001 y SGCN ISO 22301, miembro del Comité CTN320 de Ciberseguridad y Privacidad.

Profesor de los programas de formación de AENOR de gestión de la seguridad de la información ISO 27002 e ISO 27001, y de sistemas de gestión de continuidad de negocio. Ha formado a más de 3000 personas en ISO 27000 en España, México, Venezuela y El Salvador.

Imparte materia de los epígrafes: 3.3

Importe

3.800 € + IVA

Nº de asistentes

El número máximo de asistentes al programa es de 25 alumnos.

Reconocimiento

Programa reconocido por el Centro de Registro y Certificación de Personas (CERPER) para el acceso a la certificación como DPD-AEPD para candidatos sin experiencia el 24/06/2020.

Aenor Internacional, como entidad que imparte formación para la certificación de DPD, se adhiere al código ético establecido en el Esquema de certificación de delegados de protección de datos de la Agencia Española de Protección de Datos, y se compromete a cumplir los principios, valores y compromisos que en él se establen.

CERTIFICADO DE RECONOCIMIENTO

El Centro de Registro y Certificación de Personas (CERPER), entidad reconocida de forma definitiva el 26/10/2018 como Entidad de Certificación del esquema DPD-AEPD ha reconocido el programa

Experto Delegado en Protección de Datos

impartido por la entidad

Aenor Internacional S.A.U. (www.aenor.es)

como programa reconocido para el acceso a la certificación como Delegado de Protección de Datos (DPD) conforme al esquema DPD-AEPD.

Duración del programa: **180 horas**

Modalidad de impartición del programa: **mixto (online + presencial)**

Fecha del reconocimiento: **24 de junio de 2020**

Materia del programa y criterios de superación del mismo:

Sesión 1: Normativa general de protección de datos y responsabilidad activa

Sesión 2: Normativa general de protección de datos

Sesión 3: Normativa general de protección de datos y técnicas para garantizar el cumplimiento de la normativa de protección de datos

Sesión 4: Responsabilidad activa y técnicas para garantizar el cumplimiento de la normativa de protección de datos

Sesión 5: Responsabilidad activa I

Sesión 6: Responsabilidad activa II

Sesión 7: Técnicas para garantizar el cumplimiento de la normativa de protección de datos

Sesión 8: Normativa general de protección de datos

Sesión 9: técnicas para garantizar el cumplimiento de la normativa de protección de datos

Sesión 10: Normativa general de protección de datos y técnicas para garantizar el cumplimiento de la normativa de protección de datos

Sesión 11: Técnicas para garantizar el cumplimiento de la normativa de protección de datos

Proyecto final: normativa general de protección de datos y responsabilidad activa Criterios de superación del programa:

- Participación en las sesiones
- Realización de casos y ejercicios prácticos
- Participación en foros y debates
- Realización de examen
- Entrega de proyecto

Distribución de horas por cada uno de los dominios del temario del esquema DPD-AEPD:

Dominio 1: 90 horas

Dominio 2: 54 horas

Dominio 3: 36 horas

El reconocimiento mantendrá su vigencia mientras no sean modificados los requisitos verificados para su obtención de conformidad con el esquema AEPD-DPD en su versión vigente (programa, distribución por dominio, metodología docente y método de validación) o las modificaciones del propio esquema que le pudieran afectar.

La entidad de formación queda obligada al cumplimiento de los requisitos que, en relación a su actividad como entidad de formación, establezca el esquema de certificación DPD-AEPD en su versión vigente. Esto incluye el compromiso de cumplimiento por parte de la entidad de formación del código ético del esquema que figura a continuación.

El reconocimiento de esta formación no supone que la formación esté amparada por acreditación de ENAC.

ANEXO III

CÓDIGO ÉTICO PARA LAS ENTIDADES QUE SOLICITEN LA ACREDITACIÓN COMO ENTIDADES CERTIFICADORAS DE DELEGADOS DE PROTECCIÓN DE DATOS CONFORME AL ESQUEMA DE LA AGENCIA ESPAÑOLA DE PROTECCIÓN Y LAS ENTIDADES QUE OFREZCAN FORMACIÓN

PREÁMBULO

El presente Código constituye una declaración expresa de los valores y principios que, basados en la normativa aplicable y en los requisitos del Esquema de Certificación de Delegados de Protección de Datos de la Agencia Española de Protección de Datos (AEPD-DPD), deben presidir y guiar el comportamiento de aquellas entidades y empresas (en adelante, entidades interesadas) que soliciten de la Entidad Nacional de Acreditación (ENAC) la acreditación para ser entidades certificadoras (en adelante, EC) de Delegados de Protección de Datos, conforme al Esquema AEPD-DPD, en el ejercicio y desempeño de su actividad profesional.

El código ético recoge un conjunto de principios y valores (legalidad, integridad, honorabilidad, competencia leal, profesionalidad, responsabilidad, imparcialidad, transparencia y confidencialidad) que provienen de las obligaciones que establecen las distintas normativas que son de aplicación a la actividad de las entidades que solicitan la acreditación de EC a ENAC, así como de las recogidas en el Esquema AEPD-DPD.

Su observancia se fundamenta en la diligencia debida para su cumplimiento con la finalidad de proporcionar confianza y garantía de un comportamiento absolutamente responsable con la legalidad vigente en sus relaciones con empleados, proveedores, clientes y cualesquiera terceros con los que se relacionen, tanto de ámbito público como privado, incluyendo la sociedad en general.

El objetivo del presente código es procurar un comportamiento profesional por parte de las entidades interesadas: de sus directivos, empleados, apoderados, representantes y colaboradores, que se aleje de conductas y hechos contrarios a los principios y valores que recoge.

El código ético, que las entidades interesadas vienen obligadas a suscribir con carácter previo a la presentación de la solicitud de acreditación, implica el compromiso de actuar conforme a sus

principios y valores durante el procedimiento de acreditación como EC por ENAC y durante el ejercicio de su actividad como EC una vez que como tal hayan sido reconocidas.

Para que el código sea efectivo y proporcione confianza y seguridad a los que se relacionen o hayan de relacionarse con las entidades interesadas de un comportamiento ético, éstas han de proceder a su difusión entre directivos, empleados, apoderados, representantes y colaboradores; establecer procedimientos y estructuras para la comunicación y gestión de reclamaciones; y para la supervisión y control de su observancia, funciones que, en su caso, también podrán ser realizadas por la AEPD en garantía del buen funcionamiento del Esquema AEPD-DPD.

El código ético se aplica igualmente a las entidades de formación, cuyo comportamiento en el marco del Esquema AEPD-DPD ha de observar los principios y valores que contiene.

ARTÍCULO I. AMBITO DE APLICACIÓN

Los principios y valores contenidos en el presente código ético son de obligada observancia y cumplimiento para las entidades que soliciten de la Empresa Nacional de Acreditación (ENAC) ser acreditadas para certificar DPD con arreglo al Esquema AEPD-DPD, así como por sus directivos, empleados, apoderados, representantes y colaboradores, desde el mismo momento de presentación de la solicitud y durante el ejercicio de su actividad como EC en el marco del Esquema AEPD-DPD.

Será de aplicación para todas las sociedades que formen parte de las entidades interesadas, incluyendo sus directivos, empleados, apoderados, representantes y colaboradores.

El código ético será de aplicación a las entidades de formación, a sus directivos, empleados, apoderados, representantes y colaboradores.

ARTÍCULO II. PRINCIPIOS DE ACTUACIÓN

Las entidades interesadas y sus sociedades, sus directivos, empleados, apoderados, representantes y apoderados en el ejercicio de sus actividades se comportarán con sujeción a los siguientes principios:

- **Legalidad**, las entidades interesadas cumplirán estrictamente con la legislación y la normativa vigente en cada momento, y especialmente con lo establecido en el

Esquema AEPD-DPD, al objeto de evitar que se lleve a cabo cualquier actividad ilícita y, en particular, las prácticas o declaraciones que de cualquier manera supongan un perjuicio para la ENAC, AEPD, el Esquema AEPD-DPD, o a cualquiera de sus actores.

Las entidades interesadas se comprometen a adoptar las medidas necesarias para que sus directivos, empleados, apoderados, representantes y colaboradores conozcan la normativa aplicable, incluidos los principios y valores del código ético y los puedan observar.

- **Integridad,** las entidades interesadas desarrollarán sus actividades de en todo momento con ética profesional, de manera honrada, profesional y de buena fe, evitando los conflictos de intereses.

- **Honorabilidad,** las entidades interesadas no deberán haber sido objeto de sanción en cualquiera de los ámbitos de su actividad y ejercicio profesional durante los tres (3) años anteriores a la presentación de la solicitud de acreditación, ni ser sancionadas durante su desempeño como EC**.**

- **Competencia leal**, las entidades interesadas desarrollarán su actividad profesional de manera leal, sin permitir comportamientos engañosos, fraudulentos, o maliciosos.

  En protección de datos evitarán las prácticas agresivas como:

  Actuar con intención de suplantar la identidad de la Agencia Española de Protección de Datos o de una autoridad autonómica de protección de datos en la realización de cualquier comunicación a los responsables y encargados de los tratamientos o a los interesados.

  Generar la apariencia de que se está actuando en nombre, por cuenta o en colaboración con la Agencia Española de Protección de Datos o una autoridad autonómica de protección de datos en la realización de cualquier comunicación a los responsables y encargados de los tratamientos en que la remitente ofrezca sus productos o servicios.

  Realizar prácticas comerciales en las que se coarte el poder de decisión de los destinatarios mediante la referencia a la posible imposición de sanciones por incumplimiento de la normativa de protección de datos personales.

Ofrecer cualquier tipo de documento por el que se pretenda crear una apariencia de cumplimiento de las disposiciones de protección de datos de forma complementaria a la realización de acciones formativas sin haber llevado a cabo las actuaciones necesarias para verificar que dicho cumplimiento se produce efectivamente.

Asumir, sin designación expresa del responsable o el encargado del tratamiento, la función de delegado de protección de datos y comunicarse en tal condición con la Agencia Española de Protección de Datos o las autoridades autonómicas de protección de datos.

- **Responsabilidad**, en el desarrollo de sus actividades profesionales, las entidades interesadas asumirán las actividades de colaboración que le requiera la AEPD y demás autoridades públicas, así como el resto de las entidades del Esquema AEPD-DPD para su correcto desarrollo y mantenimiento, evitando cualquier conducta que perjudique su reputación.

- **Imparcialidad**, las entidades interesadas actuarán con objetividad en sus relaciones con terceros, sin aceptar presiones o influencias de terceros que pudieran cuestionar su integridad profesional, o la de sus directivos, empleados, apoderados, representantes y colaboradores, en particular con las entidades de formación del Esquema AEPD -DPD.

- **Transparencia**, las entidades interesadas actuarán con transparencia en el ejercicio de su actividad profesional, en concreto en el ámbito del Esquema AEPD-DPD que exige:

    - Informar a todas las partes interesadas de forma clara, precisa y suficiente de todos los aspectos que confluyen en el ejercicio profesional como EC, siempre y cuando los mismos no estén sujetos al régimen de confidencialidad, en cuyo caso tendrán carácter reservado y no podrán ser divulgados.

    - Facilitar a todas las partes interesadas con claridad, precisión y suficiencia toda la información relevante sobre el proceso de certificación y sobre el estado de la acreditación

- **Confidencialidad**, las entidades interesadas respetarán y guardarán la necesaria protección y reserva de la información a la que pudiera tener acceso por razón de su actividad como EC, salvaguardando los derechos legítimos de todas las partes

interesadas. Dicha información no será utilizada para su beneficio ni de su personal, ni revelada a partes inapropiadas.

ARTÍCULO III. RELACIONES CON EL PERSONAL DE LA ORGANIZACIÓN

En sus relaciones con sus empleados, directivos y colaboradores, las entidades interesadas:

- Pondrán los medios necesarios para comunicar y difundir el código ético entre todos sus empleados.
- Evitarán las situaciones que puedan dar lugar a conflictos de intereses con las actividades de la organización.
- Establecerán procedimientos que permitan la notificación de conductas contrarias al código ético y al esquema AEPD-DPD.
- Vigilarán que el personal a su cargo no lleve a cabo actividades ilícitas ni conductas contrarias al código ético y al Esquema AEPD-DPD.
- Asumirán la responsabilidad de la actuación de sus directivos, empleados apoderados, representantes y colaboradores.

ARTÍCULO IV. RELACIONES CON COLABORADORES EXTERNOS, PROVEEDORES Y CLIENTES

Las entidades interesadas:

- Establecerán unas relaciones basadas en el respeto a la legalidad vigente, el Esquema AEPD-DPD, el comportamiento ético, la lealtad, la buena fe, la confianza, respeto y transparencia.
- Actuarán con imparcialidad y objetividad en los procesos de selección de colaboradores, aplicando criterios debidamente documentados de competencia y calidad, evitando en todo momento la colisión de intereses, en particular con las entidades de formación.
- Garantizarán documentalmente una absoluta independencia con las entidades que presten formación a los candidatos a obtener la certificación.
- Darán a conocer el contenido del presente código deontológico.

ARTÍCULO V. RELACIONES CON CLIENTES

En sus relaciones con los clientes, las entidades interesadas:

- Darán a conocer el contenido del presente código deontológico.
- Actuarán de forma ética, íntegra, de buena fe y profesional, teniendo como objetivo la consecución de un alto nivel de calidad en la prestación de sus servicios, buscando el desarrollo de unas relaciones basadas en la confianza, seguridad y en el respeto mutuo.
- Salvaguardarán siempre la independencia, evitando que su actuación profesional se vea influida por vinculaciones económicas, familiares y de amistad con los clientes, o de sus relaciones profesionales al margen de la actividad de las EC, no debiendo aceptar regalos o favores de cualquier naturaleza de parte de éstos o de sus representantes.
- No efectuarán ni aceptarán, directa ni indirectamente, ningún pago o servicio de más valor ni distinto al establecido para el servicio proporcionado.
- Pondrán en conocimiento del cliente cualquier situación que pueda dar lugar a un conflicto de intereses en la prestación de sus servicios antes de asumir un encargo profesional.
- No realizarán ninguna actividad promocional (publicidad, material informativo, u otra) que pueda inducir a los clientes a una incorrecta interpretación del significado de la Acreditación bajo el Esquema AEPD-DPD, o a unas expectativas que no respondan a la situación real.
- No ofrecerán la formación requerida en el Esquema AEPD-DPD ni publicitarán, en su página web, o en otros medios, cursos relacionados con el Esquema AEPD-DPD.
- No realizarán ofertas, descuentos u otros beneficios a los candidatos a obtener la certificación como DPD por provenir de programas de formación determinados.

ARTÍCULO VI. RELACIÓN CON LAS AUTORIDADES Y ORGANISMOS PÚBLICOS

Las relaciones con las instituciones, organismos y Administraciones públicas (estatal, autonómicas y locales), especialmente con la AEPD, se desarrollarán bajo el principio de máxima colaboración y escrupuloso cumplimiento de sus resoluciones. Las comunicaciones, requerimientos y solicitudes de información que las entidades interesadas reciban de autoridades y organismos públicos deberán ser atendidas con diligencia, en los plazos establecidos para ello.

ARTÍCULO VII. CONTROL DE APLICACIÓN DEL CÓDIGO

Las Entidades de Certificación y de Formación permitirán el acceso al registro de las reclamaciones relacionadas con el código ético a ENAC y a la AEPD y colaborarán plenamente con cualquier actuación o investigación sobre su cumplimiento se lleve a cabo por ENAC o la AEPD.

ARTÍCULO VIII. ACEPTACIÓN E INTERPRETACIÓN DEL CÓDIGO ÉTICO

El Esquema AEPD-DPD exige a las entidades interesadas un alto nivel de compromiso en el cumplimiento del código ético.

Las entidades interesadas se comprometen a la suscripción y aplicación del presente código ético que forma parte del Esquema AEPD-DPD.

Cualquier duda que pueda surgir sobre la interpretación o aplicación del código ético deberá consultarse con la AEPD, quien tiene la obligación de fomentar el conocimiento y cumplimiento del código e interpretarlo en caso de duda.

ARTÍCULO IX. INCUMPLIMIENTO DEL CÓDIGO ÉTICO

La falta de adhesión al código ético, o el incumplimiento de alguno de los compromisos que implica supondrán la resolución del contrato de uso de la Marca.

ARTÍCULO X. RÉGIMEN TRANSITORIO

Las entidades interesadas y aquellas que ya estén acreditación como Entidades de Certificación por ENAC, y las Entidades de Formación deberán suscribir el código ético en los plazos que se establecen en la Disposición Transitoria del Esquema (apartado 10 del Esquema).

Aenor Internacional SAU, como entidad que imparte formación para la certificación de DPD, se adhiere al código ético establecido en el Esquema de certificación de delegados de protección de datos de la Agencia Española de Protección de Datos, y se compromete a cumplir los principios, valores y compromisos que en él se establen.