

El presente curso de Delegado de Protección de Datos (180h) tiene como objetivo capacitar tanto a los profesionales de la privacidad como a los responsables en este ámbito de las entidades que tratan los datos personales de terceros.

El curso va dirigido tanto a profesionales de privacidad, como a empresarios, responsables de organizaciones asociativas o personas interesadas en conocer todos los derechos que les otorga el Reglamento sobre el tratamiento de sus datos personales.

Así pues, con esta formación se pretende:

- Conocer los cambios introducidos en el nuevo Reglamento General de Protección de Datos, así como las obligaciones que adquieren los responsables y los encargados del tratamiento de datos personales.
- Tener conocimiento de los nuevos derechos que el RGPD incluye, así como las excepciones que el propio derecho marca.
- Entender los principales objetivos que quiere alcanzar el RGPD con estos nuevos cambios introducidos.
- Conocer la función del Delegado de Protección de Datos: características, la toma de decisiones, sus habilidades, etc.
- Elaborar las cláusulas legales necesarias para recoger datos personales cumpliendo la nueva normativa europea.
- Estar al tanto de las técnicas necesarias para garantizar el cumplimiento de la normativa de protección de datos.

## I. NORMATIVA GENERAL (90h)

### UNIDAD 1. NORMATIVA GENERAL DE PROTECCIÓN DE DATOS

#### 1.1. Contexto normativo

##### 1.1.1. Privacidad y protección de datos en el panorama internacional

##### 1.1.2. La protección de datos en Europa

##### 1.1.3. La protección de datos en España

##### 1.1.4. Estándares y buenas prácticas

#### 1.2. Fundamentos del Reglamento Europeo de Protección de Datos (RGPD)

##### 1.2.1. Ámbito de aplicación

##### 1.2.2. Definiciones

##### 1.2.3. Sujetos obligados

#### 1.3. Principios del RGPD (10h)

##### 1.3.1. El binomio derecho/deber en la protección de datos

###### 1.3.1.1. El deber de informar

##### 1.3.2. Licitud del tratamiento

##### 1.3.3. Lealtad y transparencia

##### 1.3.4. Limitación de la finalidad

##### 1.3.5. Minimización de datos

##### 1.3.6. Exactitud

### UNIDAD 2. LA LEGITIMACIÓN PARA EL TRATAMIENTO DE DATOS PERSONALES EN EL NUEVO RGPD

#### 2.1. El consentimiento: otorgamiento y revocación

##### 2.1.1. Características y condiciones del consentimiento

##### 2.1.2. ¿Qué sucede con aquellos tratamientos que se realizarán con base en el consentimiento por omisión?

##### 2.1.3. ¿En qué situaciones el consentimiento tiene que ser explícito?

#### 2.2. El consentimiento informado: finalidad, transparencia, conservación, información y deber de comunicación al interesado

##### 2.2.1. Ejemplos de consentimiento válido

##### 2.2.2. ¿Dónde almacenar ese consentimiento?

- 2.3. Consentimiento de los niños
- 2.4. Categorías especiales de datos
  - 2.4.1. Tratamiento de categorías especiales de datos
- 2.5. Datos relativos a infracciones y condenas penales
- 2.6. Tratamiento que no requiere identificación
- 2.7. Bases jurídicas distintas del consentimiento

### UNIDAD 3. DERECHOS DE LOS INDIVIDUOS

- 3.1. Transparencia e información
- 3.2. Acceso, rectificación y supresión (olvido)
- 3.3. Oposición
- 3.4. Decisiones individuales automatizadas
- 3.5. Portabilidad
- 3.6. Limitación del tratamiento
- 3.7. Excepciones a los derechos
- 3.8. Archivo multimedia: "¿Qué es exactamente el derecho al olvido?"

### UNIDAD 4. MEDIDAS DE CUMPLIMIENTO

- 4.1. Las políticas de protección de datos
- 4.2. Posición jurídica de los intervinientes. Responsables, co-responsables, encargados, subencargados del tratamiento y sus representantes. Relaciones entre ellos y formalización
- 4.3. El registro de actividades de tratamiento: identificación y clasificación del tratamiento de datos
  - 4.3.1. Registro de actividades: obligaciones
  - 4.3.2. Fases de la construcción del registro de actividades
- 4.4. Responsabilidad proactiva como nueva exigencia del RGPD
  - 4.4.1. Privacidad desde el diseño y por defecto
  - 4.4.2. Evaluación de impacto relativa a la protección de datos y consulta previa
  - 4.4.3. Seguridad de los datos personales. Seguridad técnica y organizativa
  - 4.4.4. Las violaciones de la seguridad. Notificación de violaciones de seguridad
    - 4.4.4.1. Cuestiones acerca de la notificación de seguridad
  - 4.4.5. El Delegado de Protección de Datos (DPD). Marco normativo
  - 4.4.6. Códigos de conducta y certificaciones

### UNIDAD 5. DELEGADOS DE PROTECCIÓN DE DATOS (DPD, DPO O DATA PRIVACY OFFICER)

- 5.1. Designación. Proceso de toma de decisión. Formalidades en el nombramiento, renovación y cese. Análisis de conflicto de intereses
- 5.2. Obligaciones y responsabilidades. Independencia, Identificación y reporte a dirección
- 5.3. Procedimientos. Colaboración, autorizaciones previas, relación con los interesados y gestión de reclamaciones
- 5.4. Comunicación con la autoridad de protección de datos
- 5.5. Competencia profesional. Negociación. Comunicación. Presupuestos
- 5.6. Formación
- 5.7. Habilidades personales, trabajo en equipo, liderazgo, gestión de equipos

### UNIDAD 6. TRANSFERENCIAS INTERNACIONALES DE DATOS. LAS AUTORIDADES DE CONTROL. DIRECTRICES DE INTERPRETACIÓN DEL RGPD

- 6.1. Transferencias internacionales
  - 6.1.1. El sistema de decisiones de adecuación
  - 6.1.2. Transferencias mediante garantías
  - 6.1.3. Normas Corporativas Vinculantes o BCR
  - 6.1.4. Excepciones
  - 6.1.5. Procedimiento de Autorización de Transferencias Internacionales

- 6.1.6. Suspensión temporal
- 6.1.7. Cláusulas contractuales
- 6.2. Las Autoridades de Control
  - 6.2.1. Potestades
  - 6.2.2. Régimen sancionador
  - 6.2.3. Comité Europeo de Protección de Datos
  - 6.2.4. Procedimientos seguidos por la AEPD
  - 6.2.5. La tutela jurisdiccional
  - 6.2.6. El derecho de indemnización
- 6.3. Directrices de interpretación del RGPD
  - 6.3.1. Guías del GT art. 29
  - 6.3.2. Opiniones del Comité Europeo de Protección de Datos
  - 6.3.3. Criterios de órganos jurisdiccionales

## UNIDAD 7. NORMATIVAS SECTORIALES. NORMATIVA ESPAÑOLA Y EUROPEA CON IMPLICACIONES EN PROTECCIÓN DE DATOS

- 7.1. Normativas sectoriales afectadas por la protección de datos
  - 7.1.1. Sanitaria, Farmacéutica, Investigación
  - 7.1.2. Protección de los menores
  - 7.1.3. Solvencia Patrimonial
  - 7.1.4. Telecomunicaciones
  - 7.1.5. Videovigilancia
  - 7.1.6. Seguros
  - 7.1.7. Publicidad
- 7.2. Normativa española con implicaciones en protección de datos
  - 7.2.1. LSSI, Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico
  - 7.2.2. LGT, Ley 9/2014, de 9 de mayo, General de Telecomunicaciones
  - 7.2.3. Ley firma-e, Ley 59/2003, de 19 de diciembre, de firma electrónica
- 7.3. Normativa europea con implicaciones en protección de datos
  - 7.3.1. Directiva e-Privacy: Directiva 2002/58/CE del Parlamento Europeo y del Consejo de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre privacidad y las comunicaciones electrónicas) o Reglamento e-Privacy cuando se apruebe
  - 7.3.2. Directiva 2009/136/CE del Parlamento Europeo y del Consejo, de 25 de noviembre de 2009, por la que se modifican la Directiva 2002/22/CE relativa al servicio universal y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas, la Directiva 2002/58/CE relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas y el Reglamento (CE) nº 2006/2004 sobre la cooperación en materia de protección de los consumidores
  - 7.3.3. Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo

## II. RESPONSABILIDAD ACTIVA (54h)

### UNIDAD 8. ANÁLISIS Y GESTIÓN DE RIESGOS DE LOS TRATAMIENTOS DE DATOS PERSONALES

- 8.1. Introducción. Marco general y evaluación de riesgos. Conceptos generales
- 8.2. Evaluación de riesgos. Inventario y valoración de amenazas. Salvaguardas existentes y valoración de su protección. Riesgo resultante
  - 8.2.1. Inventario y valoración de activos
  - 8.2.2. Inventario y valoración de amenazas
  - 8.2.3. Salvaguardas existentes y valoración de su protección
  - 8.2.4. Riesgo resultante

- 8.3. Gestión de riesgos. Conceptos, implementación, selección y asignación de salvaguardas a amenazas
- 8.3.1. Valoración de la protección. Riesgo residual, riesgo aceptable y riesgo inasumible
- 8.4. Metodología de análisis y gestión de riesgos
- 8.5. Programa de cumplimiento de Protección de Datos y Seguridad en una organización
- 8.5.1. El Diseño y la implantación del programa de Protección de Datos en el contexto de la organización
- 8.5.2. Objetivos del programa de cumplimiento
- 8.5.3. Accountability: La trazabilidad del modelo de cumplimiento

## UNIDAD 9. SEGURIDAD DE LA INFORMACIÓN

- 9.1. Marco normativo. Esquema Nacional de Seguridad y directiva NIS: Directiva (UE) 2016/1148 relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión
- 9.1.1. Objetivo
- 9.1.2. Requisitos
- 9.1.3. Elementos principales
- 9.1.4. Principios
- 9.1.5. Ámbito de aplicación
- 9.2. Ciberseguridad y Gobierno de la Seguridad de la Información.
- 9.2.1. Generalidades
- 9.2.2. El Gobierno efectivo de seguridad de la Información (SI)
- 9.2.3. Misión
- 9.2.4. Conceptos de SI
- 9.2.5. Alcance
- 9.2.6. Métricas de gobierno de la SI
- 9.2.7. Estado de la SI
- 9.2.8. Estrategia de SI
- 9.3. Puesta en práctica de la Seguridad de la Información
- 9.3.1. Seguridad desde el diseño y por defecto
- 9.3.2. El ciclo de vida de los sistemas de información
- 9.3.3. Integración de la seguridad y la privacidad en el ciclo de vida
- 9.3.4. El control de calidad de los SI

## UNIDAD 10. EVALUACIÓN DE IMPACTO DE PROTECCIÓN DE DATOS "EIPD"

- 10.1. Introducción y fundamentos de las EIPD: Origen, concepto y características de las EIPD
- 10.1.1. Alcance y necesidad. Estándares
- 10.2. Realización de una evaluación de impacto
- 10.2.1. Aspectos preparatorios y organizativos
- 10.2.2. Análisis de la necesidad de llevar a cabo la evaluación y consultas previas

## III. TÉCNICAS PARA GARANTIZAR EL CUMPLIMIENTO DE LA NORMATIVA DE PROTECCIÓN DE DATOS

### UNIDAD 11. LA AUDITORÍA DE PROTECCIÓN DE DATOS. AUDITORÍA DE SISTEMAS DE INFORMACIÓN

- 11.1. La Auditoría de Protección de Datos
- 11.1.1. El proceso de auditoría. Cuestiones generales y aproximación a la auditoría. Características básicas de la Auditoría
- 11.1.2. Elaboración del informe de auditoría. Aspectos básicos e importancia del informe de auditoría
- 11.1.3. Ejecución y seguimiento de acciones correctoras
- 11.2 Auditoría de Sistemas de Información
- 11.2.1. La Función de la Auditoría en los Sistemas de Información. Conceptos básicos. Estándares y Directrices de Auditoría de SI
- 11.2.2. Control interno y mejora continua. Buenas prácticas. Integración de la auditoría de protección de datos en la auditoría de SI
- 11.2.3. Planificación, ejecución y seguimiento

### 11.3. La gestión de la seguridad de los tratamientos

11.3.1. Esquema Nacional de Seguridad, ISO/IEC 27001:2013 (UNE ISO/IEC 27001:2014: Requisitos de Sistemas de Gestión de Seguridad de la Información, SGSI)

11.3.2. Gestión de la Seguridad de los Activos. Seguridad lógica y en los procedimientos. Seguridad aplicada a las TI y a la documentación

11.3.3. Recuperación de desastres y Continuidad del Negocio. Protección de los activos técnicos y documentales. Planificación y gestión de la Recuperación de Desastres

## UNIDAD 12. OTROS CONOCIMIENTOS

### 12.1. El cloud computing

12.1.1. Cómo cumplir el RGPD con cloud computing

12.1.2. Novedades a la hora de tratar los datos en Cloud con el RGPD

### 12.2. Los Smartphones

12.2.1. Principales riesgos para los usuarios finales

12.2.2. ¿Qué se debe hacer para garantizar la seguridad de los usuarios?

### 12.3. Internet de las cosas (IoT)

12.3.1. Principios del RGPD en relación con el Internet de las Cosas

### 12.4. Big data y elaboración de perfiles

12.4.1. Principios para el tratamiento masivo de datos

12.4.2. ¿Cuándo no será de aplicación el RGPD en los tratamientos de Big Data?

12.4.3. Archivo multimedia: "¿Cómo afecta el nuevo Reglamento General de Protección de Datos al Big Data?"

### 12.5. Redes sociales

12.5.1. Cambios en las políticas de privacidad de Facebook

12.5.2. Cambios en las políticas de privacidad en WhatsApp e Instagram

12.5.3. Cambios en las políticas de privacidad de Google (Gmail, Youtube, Google+)

12.5.4. Cambios en las políticas de privacidad de Twitter y LinkedIn

12.5.5. Cómo afecta el RGPD a los blogs

### 12.6. Tecnologías de seguimiento de usuario

### 12.7. Blockchain y últimas tecnologías

12.7.1. ¿Cumple el Blockchain con la normativa europea de protección de datos?

12.7.2. Preceptos en los que el Blockchain no cumple con el RGPD