

RGPD Y LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES Y GARANTÍA DE LOS DERECHOS DIGITALES

REF: K099

OBJETIVOS

- Aplicar los principios fundamentales de la protección de datos en su organización, así como las novedades que introduce el **REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS EUROPEO Y LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES Y GARANTÍA DE LOS DERECHOS DIGITALES**.
- Asignar las responsabilidades de cada uno de los sujetos que participan en el tratamiento de datos personales en la empresa. Y aprender a realizar un Registro de actividades de tratamiento, tanto para el responsable como para el encargado de tratamiento.
- Conocer cuáles son las empresas que deben nombrar un delegado de protección de datos y cuáles son sus obligaciones. Introducción al esquema de certificación del delegado de protección de datos.
- Saber cuáles son las organizaciones obligadas a realizar una evaluación de impacto y llevarla a la práctica.
- Establecer las medidas necesarias para proteger los derechos de los titulares de los datos personales y permitirles ejercerlos en función del tipo de riesgo o amenaza a la que se expone la organización en función de su sector o actividad, previa evaluación de impacto.
- Aplicar la protección de datos en los contratos de servicios que firme la empresa con sus proveedores de servicios.
- Distinguir las operaciones de cesión de datos y aplicar los requisitos que la ley establece para realizarlas.
- Establecer los requisitos necesarios para proteger los datos personales en la gestión de los recursos humanos.
- Aprender cuáles son los tipos de infracciones y sanciones a las que se expone la empresa, en caso de no aplicar de forma adecuada la normativa de protección de datos.
- Conocer cuestiones específicas como son el tratamiento de morosos o de la publicidad desde el respeto y la protección de los datos personales o la protección de datos en el departamento de recursos humanos, además de las características de determinados sectores como son las cadenas hoteleras, las comunidades de vecinos, etc.
- Aplicar los principios de protección de datos a la videovigilancia.

ÍNDICE DE CONTENIDOS

1. INTRODUCCIÓN

- 1.1. Introducción.
- 1.2. Normativa y ámbito de aplicación.
- 1.3. Procedencia de los datos de carácter personal.
- 1.4. Recogida de datos: derecho y deber de información.
- 1.5. Tratamiento basado en el consentimiento del afectado.
- 1.6. Categorías especiales de datos.
- 1.7. Inexactitud de los datos.
- 1.8. Responsabilidad activa o proactiva.
- 1.9. Deber de confidencialidad.

2. CONCEPTOS BÁSICOS. SUJETOS QUE INTERVIENEN EN LA PROTECCIÓN DE DATOS

- 2.1. Conceptos básicos.
- 2.2. Sujetos que intervienen en la protección de datos.
- 2.3. Autoridades de control: Agencia española de protección de datos y Agencias autonómicas.
- 2.4. Responsable del tratamiento.
- 2.5. Responsable de seguridad de la información.
- 2.6. Encargado del tratamiento.
- 2.7. Afectado o interesado.

- 2.7.1. Menores.
- 2.7.2. Personas fallecidas.
- 2.8. Otros: usuario, tercero, representante.
- 3. DELEGADO DE PROTECCIÓN DE DATOS (DPO)**
 - 3.1. Delegado de protección de datos.
 - 3.2. Entidades que deben nombrar un delegado de protección de datos.
 - 3.3. Funciones.
 - 3.4. Obligaciones.
 - 3.5. Cualificación del delegado de protección de datos.
 - 3.6. Esquema de certificación de delegados de protección de datos de la agencia española de protección de datos (esquema AEPD-DPD).
 - 3.7. Información sobre personas certificadas.
- 4. OBLIGACIONES Y DERECHOS EN MATERIA DE PROTECCIÓN DE DATOS**
 - 4.1. Obligaciones de la LOPD.
 - 4.1.1. Información en la recogida de datos.
 - 4.1.2. Consentimiento del afectado.
 - 4.1.3. Registro de actividades de tratamiento.
 - 4.1.4. Inventario público actividades tratamientos
 - 4.2. Derechos de las personas.
 - 4.2.1. Derecho de oposición.
 - 4.2.2. Derecho de acceso.
 - 4.2.3. Derecho a la portabilidad de datos.
 - 4.2.4. Derecho de rectificación.
 - 4.2.5. Derecho de limitación del tratamiento.
 - 4.2.6. Derecho de supresión o derecho al olvido.
 - 4.2.7. Derecho a no participar en decisiones individuales automatizadas, incluida la elaboración de perfiles.
 - 4.2.8. Derecho a Indemnización.
 - 4.2.9. Derechos de los ciudadanos ante las AA.PP.
- 5. CESIÓN DE DATOS**
 - 5.1. Qué se considera cesión o comunicación.
 - 5.2. Comunicación de datos entre Administraciones Públicas.
 - 5.3. Prestaciones de servicios.
- 6. EVALUACIÓN DE IMPACTO**
 - 6.1. Introducción.
 - 6.2. Quien realiza la evaluación de impacto.
 - 6.3. Obligación de realizar una evaluación de impacto según el RGPD.
 - 6.4. Obligación de realizar evaluación de impacto según la AEPD.
 - 6.4.1. Conforme al procedimiento utilizado en el tratamiento.
 - 6.4.2. Conforme al tipo de datos o sujetos cuya información.
 - 6.4.3. Ejemplo, resumen tratamientos necesitan evaluación.
 - 6.4.4. Resumen de situaciones en que es necesaria una evaluación de impacto.
 - 6.4.5. Cuestionario para saber si tenemos que realizar una evaluación de impacto.
 - 6.5. Etapas y actividades que realizar.
 - 6.6. Contexto.
 - 6.6.1. Ciclo de vida de los datos.
 - 6.6.2. Análisis de la legitimación o licitud del tratamiento y de la necesidad y proporcionalidad del tratamiento.
 - 6.7. Gestión de riesgos.
 - 6.8. Identificación de riesgos o amenazas.
 - 6.9. Catálogo de amenazas
 - 6.10. Evaluación del riesgo
 - 6.11. Cálculo del riesgo residual
 - 6.12. Elaboración del plan de acción y del informe de conclusiones
- 7. APLICACIÓN DE MEDIDAS TÉCNICAS Y ORGANIZATIVAS**
 - 7.1. Introducción. Diferentes tipos de medidas

- 7.2. Medidas para riesgos generales
- 7.3. Medidas para la legitimación de los tratamientos y cesiones de datos personales
- 7.4. Medidas para las transferencias internacionales
- 7.5. Medidas a aplicar a la Notificación y Registro de las Actividades de Tratamiento
- 7.6. Medidas relativas a la transparencia de los tratamientos
- 7.7. Medidas para preservar la calidad de los datos
- 7.8. Medidas aplicadas a las categorías especiales de datos
- 7.9. Medidas para salvaguardar el deber de secreto
- 7.10. Medidas de seguridad en los tratamientos por encargo
- 7.11. Medidas para preservar los derechos de los interesados
- 7.12. Medidas para preservar la seguridad en el tratamiento
- 7.13. Medidas de seguridad en el Reglamento general de protección de datos europeo
- 7.14. El documento de seguridad interno
 - 7.14.1. Procedimiento de notificación, gestión y registro de incidencias
 - 7.14.2. Identificación y autenticación
 - 7.14.3. Control de acceso
 - 7.14.4. Gestión de soportes
- 7.15. Notificación de una violación de la seguridad de los datos personales
 - 7.15.1. A la autoridad de control
 - 7.15.2. Al interesado
- 8. INFRACCIONES Y SANCIONES**
 - 8.1. Introducción.
 - 8.2. Infracciones muy graves.
 - 8.3. Infracciones graves.
 - 8.4. Infracciones leves.
 - 8.5. Sanciones.
 - 8.6. Listado de cumplimiento del RGPD
 - 8.6.1. Check list relativo al tratamiento
 - 8.6.2. Check list relativo a la protección de los derechos de los interesados
 - 8.6.3. Check list. Responsabilidad de los sujetos que participan en la gestión de la protección de datos
 - 8.6.4. Check list relativo a transferencias a países terceros u organizaciones internacionales
- 9. PROTECCIÓN DE DATOS EN DIFERENTES SECTORES DE ACTIVIDAD**
 - 9.1. Introducción.
 - 9.2. Ficheros de Recursos Humanos.
 - 9.3. Video vigilancia.
 - 9.4. Comunidades de vecinos.
 - 9.5. Telecomunicaciones.
 - 9.6. Ficheros de solvencia patrimonial y ficheros de morosos.
 - 9.7. Cadenas Hoteleras.
- 10. SUPUESTOS PRÁCTICOS**
 - Teléfonos de familiares y amigos
 - Hoja de cálculo clientes
 - Fichero manual
 - Campo observaciones
 - Fichero con fines promocionales
 - Datos de menores
 - Fichero de Curriculum
 - Información sobre cuentas bancarias
 - Prestación de servicios de Marketing
 - Ficheros de solvencia patrimonial
 - Derecho de Acceso
 - Identificación por razones de seguridad
 - Fiesta de inauguración
 - Control de Recursos Humanos

- Usuario y contraseña
- Contraseñas
- Caducidad de contraseñas
- Acceso no autorizado a su ordenador