SERVICIOS DE CONSULTORÍA EN PROTECCIÓN DE DATOS.

Adecuación del Cumplimiento con las exigencias del RGPD y a la LOPDGDD, implantando medidas de responsabilidad activa y con la diligencia debida.

Adheridos al Pacto Digital para la protección de las personas

91 109 05 11
info@controlaltsup.com
C/ Puerto de la Cruz Verde, 26. 28045 - Madrid

Base normativa y conceptual.

La protección de las personas físicas en relación con el tratamiento de datos personales es un derecho fundamental protegido por el artículo 18.4 de la Constitución española, que señala que «la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos».

En el plano legislativo, la concreción y desarrollo del derecho fundamental de protección de las personas físicas tiene lugar a nivel de la UE mediante el REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de protección de datos, RGPD).

Para adaptar el ordenamiento jurídico español al RGPD, se publicó en el BOE la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD).

Responsabilidad en las organizaciones.

El RGPD exige el cumplimiento del principio de *Accountability* o *Responsabilidad Proactiva,* el cual establece una obligación activa y sistemática del cumplimiento de la normativa de protección de datos, a través de la implantación de medidas técnicas y organizativas apropiadas.

Según la LOPDGDD y el RGPD, las organizaciones están obligadas a cumplir la normativa de protección de datos de carácter personal, lo cual incluye tanto a sociedades mercantiles tanto pymes como grandes empresas, autónomos y organismos públicos.

El RGPD identifica al responsable del tratamiento como aquella persona física o jurídica o autoridad pública encargada de decidir sobre el tratamiento de datos personales. Se encarga de determinar los fines y medios para el tratamiento, así como de establecer las medidas técnicas y organizativas que garanticen la seguridad de los datos.

El responsable del tratamiento debe ser capaz de demostrar el cumplimiento del RGPD y la LOPDGDD ante las autoridades de control.

Asimismo el RGPD identifica al encargado del tratamiento como el responsable que implica el tratamiento de datos personales por cuenta de terceros, siendo la persona física o jurídica, autoridad pública, servicio u otra entidad que presta un servicio.

Rodas las organizaciones en relación con el cumplimiento de los derechos de las personas sobre sus datos personales, tienen un responsable del tratamiento, realizan encargos de tratamiento a sus suministradores y son a su vez encargados de tratamiento de los datos de sus clientes.

Según el RGPD el responsable está obligado a aplicar medidas oportunas y eficaces y ha de poder demostrar la conformidad de las actividades de tratamiento con el Reglamento General de Protección de Datos, incluida la eficacia de las medidas.

Dichas medidas deben tener en cuenta la naturaleza, el ámbito el contexto y los fines del tratamiento así como el riesgo para los derechos y libertades de las personas físicas**.**

En qué se basa la implantación del cumplimiento.

Todas las organizaciones están obligadas a las normas reglamentarias, puesto que recogen y tratan datos de personas físicas, debiendo no solamente cumplir sino poder demostrar el cumplimiento de RGPD Y LOPDGDD.

En este sentido, entre las obligaciones que deben realizar en su organización para adaptar su actividad a las exigencias se encuentran:

- Consentimiento.

Procurar el consentimiento inequívoco, y no tácito, de los afectados para el uso de sus datos.

Es decir, la persona deberá realizar un acción afirmativa que permita tratar los datos, como por ejemplo poniendo un tick en una casilla o firmado un documento.

- Notificación de brechas de seguridad.

Está la obligación de notificar una brecha o violación de seguridad, si la misma afecta a datos personales y cuando constituya un riesgo para los derechos y las libertades de las personas físicas.

- Cláusulas de información.

Hay que dar mayor información y debe quedar claro quién trata sus datos, como los trata y por qué los trata. Principalmente se deberá informar a los afectados por el tratamiento de, al menos:

- El nombre del responsable.
- La legitimación para la recogida de los datos, es decir, el por qué podemos tratar sus datos.
- Para qué se usan.
- Cómo ejercitar los derechos.

- Plazo de conservación de los datos.

Uno de los requisitos del RGPD, en aplicación del principio de responsabilidad proactiva, es la obligación de informar del plazo de conservación de los datos.

Este capítulo requiere de análisis, ya que no existe un plazo mínimo de conservación único, sino que dependiendo del tratamiento será un periodo determinado u otro.

- Encargados de tratamiento.

Se han de incluir cláusulas de elección del proveedor que realiza servicio para la organización, por ejemplo todas aquéllas que prestan ayuda externa o asistencia técnica, tales como la empresa informática o la asesoría de tipo laboral, fiscal o contable.

Para cumplir los requisitos normativos por parte de la organización, los suministradores también deberán hacerlo.

- Registro de las Actividades de Tratamiento.

Se deben identificar los tratamientos que contengan datos de carácter personal, cada tratamiento se consideraría un registro que ha de abarcar elementos de información dicumentada en el cual se debe especificar la finalidad para que se usan esos datos tales como:

- Empleados.
- Clientes.
- Proveedores.
- Videovigilancia.
- Usuarios Web.
- Etc.

El registro de actividades de tratamiento obliga a las organizaciones a documentar los flujos de datos personales que ocurren dentro de sus procesos.

En el registro de actividades debe figurar la siguiente información:

- Identificación y datos del responsable del tratamiento de los datos, así como, en el caso de existir; del representante, del corresponsable y del DPD, Delegado de Protección de Datos.
- Finalidad del tratamiento.
- Descripción de las categorías de destinatarios.

Asimismo en aplicación del principio de responsabilidad proactiva del RGPD, este capítulo requiere de análisis, puesto que dependiendo que dependiendo del sector de actividad, tipo de relación, etc., el tratamiento tendrá una justificación y extensión u otra.

- Atención de derechos solicitados por las personas afectadas.

Estos derechos se caracterizan porque su ejercicio es gratuito, excepto si las solicitudes son manifiestamente infundadas o excesivas (por ejemplo, carácter repetitivo), las solicitudes deben responderse en el plazo de un mes, aunque, si se tiene en cuenta la complejidad y número de solicitudes, se puede prorrogar el plazo otros dos meses más y el responsable está obligado a informar sobre los medios para ejercitar estos derechos.

Si la solicitud se presenta por medios electrónicos, la información se facilitará por estos medios cuando sea posible, salvo que el interesado solicite que sea de otro modo.

Si el responsable no da curso a la solicitud, informará y a más tardar en un mes, de las razones de su no actuación y la posibilidad de reclamar ante una Autoridad de Control.

- Derecho de acceso.
- Derecho de rectificación.
- Derecho de oposición.
- Derecho de supresión ("al olvido").
- Derecho a la limitación del tratamiento.
- Derecho a la portabilidad.
- Derecho a no ser objeto de decisiones individuales automatizadas.
- Derecho de información.
- Derechos Schengen.

- DPD / DPO, Delegado de Protección de Datos.

Para ciertos tratamientos, que entrañen graves riesgos para los derechos y libertades de las personas, será obligatoria la designación de un DPO ante la AEPD.

Ejemplos de ello son las actividades públicas, las sanitarias, la enseñanza, los colegios profesionales, etc.

El DPD debe asesorar e informar a la organización sobre el cumplimiento de las exigencias del RGPD y de la LOPDGDD en su organización.

Las entidades públicas o aquéllas participadas o que realicen una función pública requieren de la designación de un DPD.

El DPD promoverá el cumplimiento normativo en base a los registros y evidencias objetivas que se encuentran documentadas en la organización, supervisando el tratamiento realizado por responsables y encargados de tratamientos de datos personales como un método básico que les va a permitir identificar la adecuación a los requisitos de cumplimiento del RGPD, con el objeto de poder valorar los aspectos que deben tener en cuenta, como por ejemplo durante los procesos de análisis de riesgos y evaluación de impacto, lo cual puede suponer una ayuda en las tareas de supervisión y asesoramiento que llevan a cabo los DPD.

- AR/ GR análisis y gestión de riesgos y EIPD, evaluación de impacto de protección de datos.

Cuando iniciemos un nuevo tratamiento, deberemos hacer un análisis previo de los riesgos que conlleva para las personas que aportan sus datos en él. Ejemplos de ello son, la puesta en marcha de una página web con formulario de contacto o el análisis estadístico, etc.

El análisis de riesgos en el RGPD es el conjunto de actividades y tareas que permiten controlar la incertidumbre relativa a una amenaza mediante una secuencia de actividades que incluyen la identificación y evaluación del riesgo, así como, las medidas para su reducción o mitigación

El RGPD establece que las medidas técnicas y organizativas apropiadas para garantizar el nivel de seguridad adecuado al riesgo se definen en función del estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento así como los riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas.

No se establecen medidas de seguridad estáticas, de forma que corresponderá al responsable determinar aquellas medidas de seguridad que son necesarias para garantizar la confidencialidad, la integridad y la disponibilidad de los datos personales.

En ciertos casos, debido al riesgo, este análisis previo deberá tomar la forma de una Evaluación de Impacto en la Protección de Datos Personales (EIPD).

La Evaluación de Impacto en la Protección de Datos Personales (en adelante, la EIPD) es una herramienta que permite evaluar de manera anticipada cuáles son los potenciales riesgos a los que están expuestos los datos personales en función de las actividades de tratamiento que se llevan a cabo con los mismos.

Ventajas de la gestión de protección de datos informatizada.

- Funciona mediante el desarrollo de las **Políticas de Protección de Datos** que se ha de aplicar en cumplimiento de las distintas exigencias que cada tratamiento requiere, estableciendo a través del software los requisitos de **RGPD y LOPDGDD**.

- Una serie de **procesos comunes**, desglosados en los siguientes Capítulos:

- **PARTE 1. OFICINA DE PROTECCIÓN DE DATOS.**

- CAPÍTULO 1. POLÍTICAS DE PROTECCIÓN DE DATOS Y PRIVACIDAD.

- CAPÍTULO 2. BUENAS PRÁCTICAS DE PROTECCIÓN DE DATOS Y PRIVACIDAD.

- CAPÍTULO 3. DERECHOS DE LAS PERSONAS SOBRE LA PROTECCIÓN DE SUS DATOS PERSONALES.

- CAPÍTULO 4. FORMULARIOS DE MEDIDAS DE CUMPLIMIENTO.

- CAPÍTULO 5. DISPOSICIONES INFORMATIVAS.

- CAPÍTULO 6. RÓTULOS INFORMATIVOS.

- **PARTE 2. EVALUACIONES Y AUDITORÍAS.**

- EVALUAVIONES INICIALES / BÁSICAS.

- AUDITORÍA DE CUMPLIMIENTO DE OBLIGACIONES LEGALES.

- AUDITORÍAS DE PROTECCIÓN DE DATOS.

- ANÁLISIS DE RIESGOS. EVALUACIONES DE IMPACTO.

- AUDITORÍAS DE CUMPLIMIENTO RGPD.

- **PARTE 3. REGISTROS Y DOCUMENTOS FIRMADOS.**

- CONTRATOS.

- ENCARGOS DE TRATAMIENTO.

- NOTIFICACIONES AEPD.

- EJERCICIO DE DERECHOS.

- QUEJAS Y RECLAMACIONES.

- OTROS DOCUMENTOS**.**

Disponibilidad 24-365.

- El Cliente recibirá tendrá acceso continuado y disponibilidad interrumpida las 24 horas al día durante los 365 días del año, para demostración del cumplimiento de **los requisitos específicos de su actividad**, así como para la adecuación a las exigencias RGPD y LOPDGG.

- Se trata de una herramienta informatizada versátil, flexible y específica, que sirve para que el Cliente reciba un servicio personalizado.

- Consta entre otros de los siguientes elementos:

  • ACCESO REMOTO AL SISTEMA DESDE CUALQUIER DISPOSITIVO.
  • INFORMACIÓN TÉCNICA Y JURÍDICA.
  • PROCEDIMIENTOS ESPECÍFICOS.
  • PROCESOS DE SU ACTIVIDAD.
  • REGISTROS DE GESTIÓN.
  • REGISTROS PROPIOS Y EXTERNOS.
  • SEGURIDAD, INTEGRIDAD, DISPONIBILIDAD Y AUTENTICIDAD.
  • CONFIDENCIALIDAD MEDIANTE ACCESOS RESTRINGIDOS.
  • CERO PAPELES -TODO EN LA NUBE.

- El Cliente está en condiciones de **demostrar su adecuación**, una vez alcanzado el nivel de cumplimiento.

- La protección de datos y la **responsabilidad activa**, resultan de fácil acceso y localización, para cualquier cuestión interna o externa de la organización.

- A través de la **plataforma tecnológica de CONTROLALTSUP**, el Cliente puede **integrar** diferentes sistemas e implantar los modelos de gestión, ya que su diseño hace más eficaz el manejo de la información documentada, mejora la planificación y la comunicación y disminuye tiempos y costos de dedicación.

- La organización puede **gestionar informáticamente todos los procesos**, integrándolos y permitiendo administrar la gestión de la producción en **cualquier tratamiento de datos personales**.

Para saber más:

GARANTE PRIVACY.
C/ Puerto de la Cruz Verde, 26. 28045 • Madrid.
Teléfono: (+34) 91 109 05 11
coordinadortecnico@garanteprivacy.es