SERVICIOS DE CONSULTORÍA EN RESPONSABILIDAD ACTIVA.

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.

Los servicios de consultoría en protección de datos personales que ofrecemos, tienen una componente importantísima en cuanto al cumplimiento de la Responsabilidad Activa, razón por la cual ofrecemos asesoramiento personalizado para adaptar la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD) a las necesidades de cada organización, en base a un conjunto de soluciones y herramientas para cada tipo de elemento a tratar y sector de actividad.

Además, se ha de contemplar con adecuada perspectiva 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), mediante nuestro servicio íntegro de asesoramiento, gestión y mantenimiento de las responsabilidades que se derivan para la organización y más concretamente, de su Responsabilidad Activa.

Responsabilidad Activa.

La Responsabilidad Activa es un principio clave tanto en la LOPDGDD, como en el RGPD.

Según la AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, este principio establece que los responsables del tratamiento de datos personales deben mantener una diligencia debida permanente para proteger y garantizar los derechos y libertades de las personas físicas cuyos datos son tratados.

Véase www.aepd.es.

La Responsabilidad Activa implica que las administraciones públicas, las empresas y los profesionales, deben adoptar medidas técnicas y organizativas que aseguren razonablemente que están en condiciones de cumplir con los principios, derechos y garantías que el RGPD y la LOPDGDD establecen.

El RGPD promueve el pensamiento basado en riegos, según el cual el principio de actuar sólo cuando ya se ha producido un incumplimiento en la protección de los datos personales, una brecha de seguridad o, lo que es aún peor, una infracción, es insuficiente como estrategia, al ser una exigencia el tener que haberse anticipado mediante la obligación de tomar dichas medidas técnicas y organizativas, para haberlo evitado.

La infracción puede causar daños a los interesados que pueden ser muy difíciles de compensar o reparar a posteriori. Dichos daños, aunque tengan su origen externo en alguno de los muy diversos problemas que a diario se presentan, es obligado para la organización anticiparse a ellos.

Por tanto, los motivos ajenos como por ejemplo el robo de datos, la suplantación de identidad o los ciberataques, no pueden eximir de la responsabilidad, ni el contexto de la organización justifica las infracciones.

En qué se basa la el cumplimiento de la Responsabilidad Activa.

El principio de Responsabilidad Activa, también denominado “responsabilidad proactiva” o “responsabilidad demostrada” según la AEPD, obliga a los responsables del tratamiento a proteger continuamente y a garantizar en todo momento los derechos y libertades de las personas físicas cuyos datos son tratados por las organizaciones.

Los riesgos que el tratamiento representa para esos derechos y libertades, han de evaluarse con carácter previo al tratamiento de los datos personales, llevando a cabo un análisis de riesgos, para anticiparse a las amenazas y los peligros y para evitar sus consecuencias.

Estas consecuencias no se materializarán o sus probabilidades de ocurrencia disminuirán hasta un valor tolerable si se adoptan salvaguardias de protección y de seguridad.

De este modo el responsable puede, tanto garantizar los derechos y libertades como estar en condiciones de demostrar que el tratamiento se ajusta a las previsiones del RGPD y la LOPDGD.

Las obligaciones del responsable en cumplimiento del principio de Responsabilidad Activa que el RGPD incorpora son las siguientes, sin perjuicio de otras que pudieran ser necesarias, para lo cual la organización recibirá información, asistencia técnica y asesoramiento por nuestra parte.

- 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 Activa del RGPD, el deber de identificar los tratamientos requiere de análisis, puesto que dependiendo del sector de actividad, tipo de relación, etc., el tratamiento tendrá una justificación y extensión u otra.

- Inventario de las Actividades de Tratamiento.

Además del registro de actividades de tratamiento, las Administraciones Públicas y más concretamente las entidades señaladas en la LOPDGDD en su artículo 77.1, con fines de transparencia (Art. 6.bis Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno), deberán hacer público el inventario de sus actividades de tratamiento de manera que sea accesible por medios electrónicos (Art. 31.2 LOPDGDD) donde se incluya, para cada actividad de tratamiento:

- el nombre y los datos de contacto del responsable y, en su caso, del corresponsable, del representante del responsable, y del delegado de protección de datos;
- la base jurídica del tratamiento;
- los fines del tratamiento;
- una descripción de las categorías de interesados y de las categorías de datos personales;
- las categorías de destinatarios a quienes se comunicaron o comunicarán los datos personales, incluidos los destinatarios en terceros países u organizaciones internacionales;
- en su caso, las transferencias de datos personales a un tercer país o una organización internacional, incluida la identificación de dicho tercer país u organización internacional y, en el caso de las transferencias indicadas en el artículo 49, apartado 1, párrafo segundo, la documentación de garantías adecuadas;
- cuando sea posible, los plazos previstos para la supresión de las diferentes categorías de datos;
- cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad.

En dicha descripción general debe evitarse cualquier información que pudiera ser perjudicial para la organización, para los tratamientos de datos personales y que comprometiese la propia seguridad.

Se recomienda contar con el Responsable de Seguridad o CISO con carácter previo a la publicación de dicha descripción general o, en su caso, utilizar una referencia general a los estándares de seguridad utilizados.

- 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 (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.

- Consulta previa.

Cuando en un tratamiento que cumpla con los principios de protección de datos, en particular el de legitimidad, el responsable identifica, tras la ejecución de la EIPD, que existen riesgos que no haya podido evitar o mitigar suficientemente, deberá realizar una consulta a la Autoridad de Control.

La consulta a la Autoridad de Control no tiene por objeto la obtención de un asesoramiento con relación a aspectos generales del cumplimiento de la normativa de protección de datos (Bases jurídicas, proporcionalidad, necesidad, minimización, información, derechos de los interesados, etc.) ni tampoco obtener la aprobación del tratamiento por parte de la Autoridad de Control.

La respuesta a la consulta previa a la Autoridad de Control tiene por objeto, orientar al responsable con relación a aquellos riesgos que no hubiera sido capaz de identificar o mitigar suficientemente.

Corresponde al responsable llevar a cabo la evaluación de los riesgos que sus tratamientos pudieran implicar para los derechos y libertades de las personas físicas en el contexto del desarrollo de la EIPD.

El contenido mínimo que debe ser tenido en cuenta para llevar a cabo una solicitud de consulta previa relativa al artículo 36 del RGPD es el que se detalla en el apartado 3 de dicho artículo. Se trata de un contenido mínimo sobre el que responsable podrá añadir la información que considere oportuna y sin perjuicio de los requerimientos que la Autoridad de Control pudiera llevar a cabo en el marco de los poderes que le otorga el artículo 58 del RGPD.

- Protección de datos desde el diseño.

El RGPD exige a los responsables establecer las medidas técnicas y organizativas necesarias a lo largo de todo el ciclo de vida del tratamiento, tanto desde el momento inicial en que se lleva a cabo la definición del tratamiento y se determinan los medios como durante su puesta en marcha y funcionamiento habitual.

Estas medidas y garantías deben establecerse atendiendo a la naturaleza, el ámbito, el contexto y los fines del tratamiento, así como a los riesgos para los derechos y libertades de los interesados que pueda llegar a representar.

La protección de datos desde el diseño tiene por objetivo aplicar los principios de protección de datos en los procesos de diseño de los sistemas y procedimientos de la organización sobre los que se apoya el tratamiento de los datos.

El fin que tiene la protección de datos desde el diseño es eminentemente preventivo y orientado tanto a evitar posibles daños a las personas físicas como, de manera colateral, los perjuicios que para la organización podría suponer la modificación o el rediseño de los sistemas en los que se llevan a cabo los tratamientos.

Este carácter preventivo tiene gran importancia una vez desarrollados e implantados dichos sistemas, como consecuencia de la identificación de errores de diseño que pudieran suponer daños o perjuicios a los interesados y a sus derechos y libertades.

- Protección de datos por defecto.

El principio de protección de datos por defecto supone la puesta en práctica del principio de minimización de datos mediante las medidas técnicas y organizativas que garanticen, por defecto, que únicamente sean objeto de tratamiento los datos necesarios para los fines del mismo y que hubieran sido definidos en la etapa de diseño inicial.

El RGPD exige del responsable una configuración por defecto de los tratamientos que sea respetuosa con los principios de protección de datos, abogando por un procesamiento mínimamente intrusivo:

- mínima cantidad de datos personales,
- mínima extensión del tratamiento,
- mínimo plazo de conservación y
- mínima accesibilidad a datos personales.

Todo ello, además, sin que sea necesaria la intervención del interesado para garantizar que estos mínimos se hayan establecido.

De ahí que la protección de datos por defecto no se limita a requisitos sobre programas o dispositivos, sino que afecta también al propio diseño del tratamiento, con independencia del soporte en el que este se desarrolle.

También deben ser tenidas en cuenta las opciones de configuración que pudieran definir la implementación concreta del tratamiento atendiendo a las decisiones que el propio interesado pudiera tomar acerca de cómo desea que sean tratados sus datos.

- Seguridad de los tratamientos.

El artículo 32 del RGPD impone a los responsables del tratamiento de datos personales la obligación de determinar y establecer las medidas de seguridad técnicas y organizativas apropiadas para garantizar el nivel de seguridad adecuado al riesgo 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.

A fin de mantener la seguridad de los tratamientos se exige al responsable evaluar los riesgos inherentes al tratamiento y aplicar medidas para mitigarlos. En dicha evaluación del riesgo deben tenerse en cuenta los riesgos que atenten contra los derechos y libertades de los interesados, especialmente sus derechos y libertades fundamentales.

Con el objetivo de seleccionar las medidas para gestionar el riesgo para los derechos y libertades, pueden utilizarse estándares de seguridad ya existentes en el mercado como la norma internacional UNE ISO/IEC 27001:2022.

Por su parte, las Administraciones Públicas deberán utilizar el Esquema Nacional de Seguridad para seleccionar las medidas que deban implantarse para evitar su pérdida, alteración o acceso no autorizado, adaptando los criterios de determinación del riesgo en el tratamiento de los datos. Con carácter general el estándar utilizado implicará:

- La realización de un inventario de activos partiendo de la descripción sistemática del tratamiento.
- La identificación de los riesgos, para los derechos y libertades de los interesados, asociados a los activos que consten en el inventario de activos.
- La evaluación del riesgo para los derechos y libertades de los interesados.
- La gestión de riesgos para los derechos y libertades de los interesados a lo largo del ciclo de vida del tratamiento.

- Notificación de brechas de datos personales a la Autoridad de Control.

Una brecha de datos personales es un incidente de seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de los datos personales tratados por un responsable, o bien la comunicación o acceso no autorizados a los mismos.

Una brecha de datos personales puede tener una serie de efectos adversos considerables en las personas, susceptibles de ocasionar daños y perjuicios físicos, materiales o inmateriales; por lo que hay que intentar evitarlas y en caso de que sucedan gestionarlas adecuadamente, especialmente cuando puedan poner en riesgo los derechos y libertades de las personas físicas.

El artículo 33 del RGPD impone a los responsables de un tratamiento de datos personales la obligación de notificar a la autoridad de control competente las brechas de datos personales cuando sea probable que constituyan un riesgo para los derechos y libertades de las personas.

El responsable de tratamiento debe valorar el nivel de riesgo de una brecha de datos personales y notificarla a la autoridad de control cuando exista tal riesgo, y además cuando el riesgo sea alto el responsable también deberá comunicar la brecha a las personas afectadas conforme al artículo 34 del RGPD.

El plazo para notificar a la autoridad de control es de 72 horas desde que la organización tiene constancia de la brecha.

En el ámbito privado, los responsables del tratamiento afectados por una brecha de datos personales deberán notificar a la AEPD:

- Cuando su único establecimiento esté localizado en España.
- Si tienen varios establecimientos en la Unión Europea, únicamente cuando el establecimiento principal esté localizado en España.
- Si no tienen establecimiento principal en la Unión Europea, sólo en el caso de que hayan designado un representante en España.
- Si no tienen establecimiento ni representante en la Unión Europea, en el caso de que la brecha de datos personales cuente con afectados en España.

En el ámbito público, con carácter general las Administraciones Públicas deben notificar las brechas de datos personales a la Agencia Española de Protección de Datos a excepción cuando las brechas de datos personales se produzcan en entidades del sector público bajo su competencia, del caso de las Comunidades Autónomas de:

- Andalucía. https://ws050.juntadeandalucia.es/vea/faces/vi/procedimientos.xhtml
- Cataluña. https://apdcat.gencat.cat/es/inici/
- País Vasco. https://www.avpd.euskadi.eus/s04-5273/es/contenidos/informacion/contacto/es_9493/es_contacto.html

Las notificaciones de brechas de datos personales a la AEPD se deben realizar de forma electrónica, usando el formulario de notificación de brechas de datos personales de la Sede Electrónica para garantizar una correcta ejecución de las obligaciones del artículo 33.3 del RGPD.

La notificación a la autoridad de control de una brecha que afecta a datos personales forma parte de la responsabilidad proactiva establecida en el RGPD, y el hecho de notificarla no implica necesariamente la apertura de un procedimiento administrativo. De hecho, notificar en tiempo y forma es una evidencia de la diligencia de la organización, mientas que no cumplir con esa obligación si está tipificado como infracción.

Sin embargo, en aquellos casos en los que el responsable considere que no existieran riesgos para los derechos y libertades de las personas físicas el responsable tiene la obligación de documentar cualquier violación de la seguridad de los datos personales, incluidos los hechos relacionados con ella, sus efectos y las medidas correctivas adoptadas, dicha documentación permitirá a la autoridad de control verificar el cumplimiento de lo dispuesto en el artículo 33 del RGPD.

- Comunicación de brechas de datos personales a los interesados.

Una brecha de datos personales puede tener una serie de efectos adversos considerables en las personas, susceptibles de ocasionar daños y perjuicios físicos, materiales o inmateriales; por lo que hay que intentar evitarlas y en caso de que sucedan gestionarlas adecuadamente, especialmente cuando puedan poner en riesgo los derechos y libertades de las personas físicas.

El artículo 34 del RGPD impone a los responsables de un tratamiento de datos personales la obligación de comunicar a las personas afectadas aquellas brechas de datos personales que puedan entrañar un riesgo alto para sus derechos y libertades.

El responsable de tratamiento debe valorar el nivel de riesgo de una brecha de datos personales y en aquellos casos en los que determine que el riesgo para los derechos y libertades de las personas pueda ser alto, deberá comunicar la brecha a los afectados y notificarla a la autoridad de control competente conforme al artículo 33 del RGPD.

La comunicación a las personas afectadas debe realizarse en un lenguaje claro y sencillo, dirigirse específicamente a aquellas personas para las que exista un riesgo alto de que sus derechos y libertades pueden verse dañados, e incluir el siguiente contenido mínimo:

- Datos de contacto del DPD, o en su caso, del punto de contacto en el que pueda obtenerse más información.
- Descripción general del incidente y momento en que se ha producido.
- Las posibles consecuencias de la brecha de datos personales.
- Descripción de los datos e información personal afectados.
- Resumen de las medidas implantadas hasta el momento para controlar los posibles daños.
- Otras informaciones útiles para que los afectados puedan proteger sus datos o prevenir posibles daños.

La comunicación preferentemente se deberá realizar de forma directa al afectado, ya sea por teléfono, correo electrónico, SMS, a través de correo postal, o a través de cualquier otro medio dirigido al afectado que el responsable considere adecuado.

Cuando la comunicación a los afectados suponga un esfuerzo desproporcionado con relación a los riesgos para los derechos y libertades que están sufriendo los interesados, se podrá realizar una comunicación indirecta a través de avisos públicos.

En tal caso, el aviso público ocupará un lugar destacado, de forma que en ningún caso pueda pasar desapercibidos.

Una comunicación incompleta (sin el contenido mínimo), de difícil acceso o realizada a las personas incorrectas no es efectiva, por lo que una comunicación en estas condiciones podría llegar a considerarse una comunicación no realizada.

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