DIPUTACIÓ DE VALÈNCIA

Protecció de Dades i Seguretat de la Informació

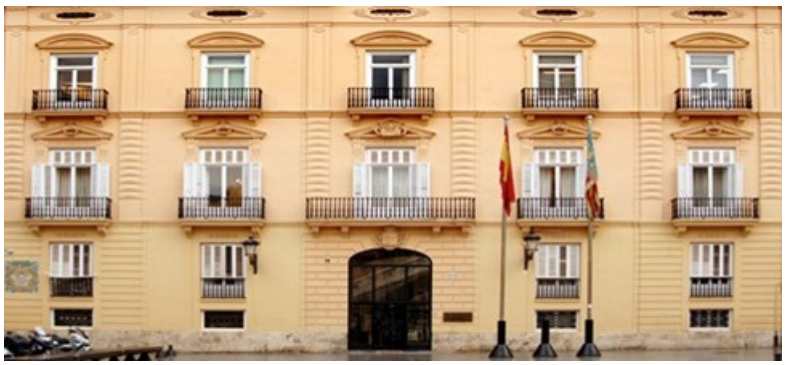
Boletín protección de datos

Boletín del Departamento de protección de datos y Seguridad de la Información de la Diputación Provincial de Valencia

Boletín N.º 17| Noviembre 2021

PRINCIPIOS BÁSICOS EN EL TRATAMIENTO DE DATOS DE CARÁCTER PERSONAL

Í N D I C E



PRINCIPIOS BÁSICOS EN EL TRATAMIENTO DE DATOS DE CARÁCTER PERSONAL Pág.

Introducción…… 3

- Principios relativos al tratamiento 4
- Responsabilidad Proactiva 5
- Medidas a tener en cuenta 7

Material complementario …… 8

Noticias de actualidad …… 8

Os invitamos a trasladarnos aquellas temáticas que resulten de vuestro interés para los próximos boletines informativos. Estas peticiones deberán dirigirse a:

Diputación de Valencia

Dpto. de Protección de Datos y Seguridad de la Información

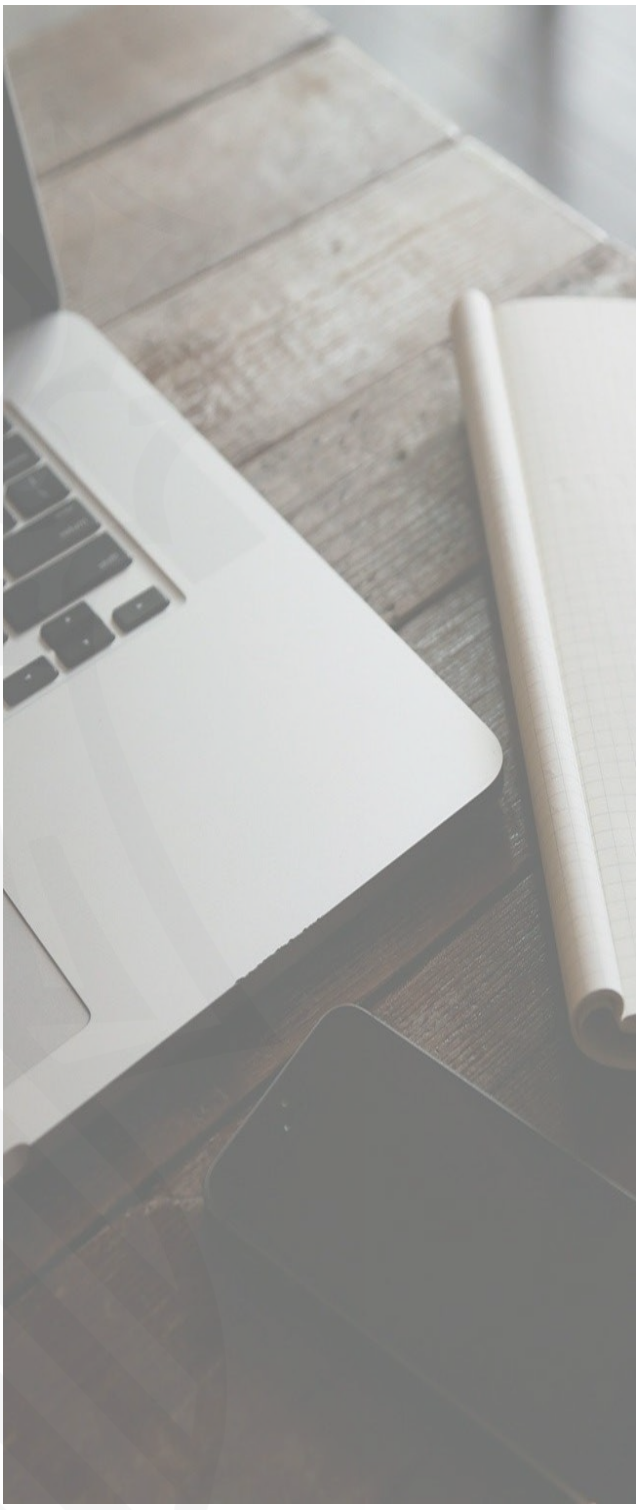
Pl. de Manises, 4 46003 Valencia

email: dpdsi@dival.es

SUSCRIPCIONES

Si deseas suscribirse a nuestro Boletín informativo accede al siguiente enlace

INTRODUCCIÓN



Existen determinados principios que deben tener presentes todas las organizaciones a la hora de tratar **nuestros datos de carácter personal**. Estos principios se encuentran regulados en el artículo 5 del Reglamento (UE) 2016/679 General de Protección de Datos (de ahora en adelante, RGPD) y, de forma conexa, en determinados preceptos de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (de ahora en adelante, LOPDGDD).

Los **principios protección de datos** son: (i) Licitud, lealtad y transparencia, (ii) Limitación de la finalidad, (iii) Minimización de los datos, (iv) Exactitud, (v) Limitación del plazo de conservación, (vi) Integridad y confidencialidad y (vii) responsabilidad Proactiva.

En este boletín vamos a analizar uno a uno los principios protección de datos y como deben ser interpretados.

Cabe destacar, que el RGPD introduce un cambio drástico en materia de responsabilidad que se proyecta sobre todas las obligaciones a las que está sometidas el Responsables del Tratamiento, se trata del principio de Responsabilidad Proactiva o accountability.

El RGPD describe este principio como la necesidad de que los responsables del tratamiento apliquen medidas técnicas y organizativas apropiadas, no sólo para garantizar el cumplimiento de la normativa, sino también para demostrar ante los interesados y autoridades de supervisión, dicho cumplimiento.

Lo cual se traduce en la exigencia de una mayor implicación por parte de los responsables y los encargados con una actitud proactiva y consciente.

PRINCIPIOS RELATIVOS AL TRATAMIENTO

Cuando hablamos de **Principios**, entendemos como tales lo que dispone el art.5 del RGPD;

"Artículo 5: Principios relativos al tratamiento

1. ***Los datos personales serán:***

a. tratados de manera ***lícita, leal y transparente*** *en relación con el interesado («****licitud, lealtad y transparencia****»);*

b. recogidos con ***fines determinados, explícitos y legítimos****, y no serán tratados ulteriormente de manera incompatible con dichos fines; de acuerdo con el artículo 89, apartado 1 (Investigación Científica, estadística), el tratamiento ulterior de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos no se considerará incompatible con los fines iniciales («****limitación de la finalidad****»);*

c. ***adecuados, pertinentes y limitados*** *a lo necesario en relación con los fines para los que son tratados («****minimización de datos****»);*

d. ***exactos*** *y, si fuera necesario****, actualizados****; se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan («****exactitud****»);*

e. ***mantenidos*** *de forma que se permita la identificación de los interesados* ***durante no más tiempo del necesario para los fines del tratamiento de los datos personales****; los datos personales podrán conservarse durante períodos más largos siempre que se traten exclusivamente con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89 (Investigación Científica, estadística), apartado 1, sin perjuicio de la aplicación de las medidas técnicas y organizativas apropiadas que impone el presente Reglamento a fin de proteger los derechos y libertades del interesado («****limitación del plazo de conservación****»);*

f. tratados de tal manera que ***se garantice una seguridad adecuada de los datos personales****, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas («****integridad y confidencialidad****»).*

2. ***El responsable del tratamiento será responsable del cumplimiento*** *de lo dispuesto en el apartado 1 y capaz de demostrarlo («****responsabilidad proactiva****»)."*

> ***Considerando 39; " Todo tratamiento de datos personales debe ser lícito y leal. Para las personas físicas debe quedar totalmente claro que se están recogiendo, utilizando, consultando o tratando de otra manera datos personales que les conciernen, así como la medida en que dichos datos son o serán tratados. El principio de transparencia exige que toda información y comunicación relativa al tratamiento de dichos datos sea fácilmente accesible y fácil de entender, y que se utilice un lenguaje sencillo y claro. Dicho principio se refiere en particular a la información de los interesados sobre la identidad del responsable del tratamiento y los fines del mismo y a la información añadida para garantizar un tratamiento leal y transparente con respecto a las personas físicas afectadas y a su derecho a obtener confirmación y comunicación de los datos personales que les conciernan que sean objeto de tratamiento. […]"***

Los principios generales de la protección de datos de carácter personal, no sólo son meros fundamentos por los que se ha de regir la elaboración, interpretación y aplicación de la normativa sobre protección de datos, sino que se trata de un conjunto de reglas que determinan cómo recoger, tratar y ceder los datos.

En caso de encontrarnos con lagunas o vacíos legales, nos hemos de inspirar en éstos, para que el tratamiento de los datos sea conforme a la normativa.

En definitiva, son deberes y obligaciones a los que están sujetos los tratamientos de datos de carácter personal.

Los principios recogidos en el RGPD [semejantes a los dispuestos en la predecesora legislación, europea y española] son como antes hemos ya adelantado, los siguientes:

" Considerando 40: Para que el tratamiento sea lícito, los datos personales deben ser tratados con el consentimiento del interesado o sobre alguna otra base legítima establecida conforme a Derecho, ya sea en el presente Reglamento o en virtud de 4.5.2016 ES Diario Oficial de la Unión Europea L 119/7 otro Derecho de la Unión o de los Estados miembros a que se refiera el presente Reglamento, incluida la necesidad de cumplir la obligación legal aplicable al responsable del tratamiento o la necesidad de ejecutar un contrato en el que sea parte el interesado o con objeto de tomar medidas a instancia del interesado con anterioridad a la conclusión de un contrato."

- Lealtad – No pueden recabarse datos personales por medios fraudulentos (esto es, no podrán utilizase medios o métodos engañosos) desleales (que den lugar a una discriminación injusta o arbitraria contra los titulares) e ilícitos (es decir, que sean ilegales, estén fuera o al margen de la Ley).
- Transparencia – Exige que toda información y comunicación relativa al tratamiento de datos personales sea fácilmente accesible y fácil de entender, y que se utilice un lenguaje sencillo y claro
- Licitud o legitimación del tratamiento.- Para que el tratamiento sea lícito, los datos personales deben ser tratados con el consentimiento explícito del interesado o sobre otra base o fundamento jurídico (artículo 6 RGPD).
- Limitación de la finalidad.- Los datos personales deben ser recogidos con fines determinados, explícitos y legítimos, y no serán tratados, posteriormente, de manera incompatible o distinta con dichos fines.
- Minimización.- Deben ser adecuados, pertinentes y limitados o no excesivos, en relación con los fines que legitiman el tratamiento.
- Exactitud- Los datos deben ser exactos y, si fuera necesario, actualizados. Deben adoptarse todas las medidas razonables para corregir errores, modificar los datos que resulten ser inexactos o incompletos y garantizar la certeza de la información objeto de tratamiento.
- Limitación del plazo de conservación.- No podrán conservarse o mantenerse los datos durante más tiempo del necesario para los fines del tratamiento. Deben establecerse plazos para la supresión o revisión periódica.
- Integridad y confidencialidad.- Debe garantizarse una seguridad adecuada para preservar la integridad de los datos e impedir el acceso o uso no autorizado. Todas las personas que intervengan en cualquier fase del tratamiento están sujetas a guardar secreto o confidencialidad con carácter indefinido

RESPONSABILIDAD PROACTIVA

Como adelantábamos en la introducción, el RGPD nos introduce el principio denominado "responsabilidad proactiva", expresión que pretende traducir el término inglés "accountability", según el cual los responsables aplicarán las medidas técnicas y organizativas apropiadas para garantizar y estar en condiciones de demostrar que el tratamiento de datos personales se lleva a cabo de conformidad con el Reglamento.

Antes de entrar a ver el principio de responsabilidad proactiva en el (RGPD), cabe indicar que el Grupo de Trabajo del Artículo 29 (GT29), que fue sustituido tras la plena aplicación del RGPD (el 25 de mayo) por el Comité Europeo de Protección de Datos (CEPD), publicó en 2010 el Dictamen 3/2010 sobre el principio de responsabilidad, WP 173, en el que explicaba su significado y alcance.

El GT29 señalaba que «proviene del mundo anglosajón donde es de uso general y donde se da una comprensión ampliamente compartida de su significado, aunque la definición exacta de «responsabilidad» resulta compleja en la práctica.» Y también que «el término apunta sobre todo al modo en que se ejercen las competencias y al modo en que esto puede comprobarse.»

Como señala la AEPD (Principio Responsabilidad Proactiva) el RGPD, en su artículo 24, describe este principio como la necesidad de que el responsable del tratamiento aplique medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el Reglamento.

Para ello las organizaciones han de analizar qué datos tratan, con qué finalidades lo hacen y qué tipo de operaciones de tratamiento llevan a cabo, para pasar a realizar el Análisis de Riesgos.

Así pues al hablar de Responsabilidad proactiva o *accountability* nos centrados en dos elementos:

1. La necesidad de que el responsable del tratamiento adopte medidas adecuadas y eficaces para aplicar los principios de protección de datos.

   Medidas técnicas y organizativas que serán revisadas y actualizadas, es decir, el responsable del tratamiento tendrá que evaluar o analizar en todo momento el riesgo, atendiendo también a cualquier cambio en el mismo ya sea, por ejemplo, por nuevos tratamientos de datos personales

2. La necesidad de demostrar, si así se requiere, que se han adoptado medidas adecuadas y eficaces. En este caso se consigue recabando evidencias, documentando actuaciones que podrán ser de prueba ante incidentes

Por último señalar que la responsabilidad proactiva se exige al responsable del tratamiento con independencia de que trate los datos personales por sí mismo o a través de un encargado del tratamiento o subencargados de tratamiento.

MEDIDAS A TENER EN CUENTA

El principio de responsabilidad proactiva o accountability pone de relieve la necesidad de dar visibilidad a las buenas prácticas en la protección de datos, lo cual se manifiesta en el artículo42 del Reglamento, pero

¿Qué medidas encontramos en el RGPD cuya aplicación supone que las organizaciones están siendo proactivas en la adopción de medidas de seguridad?

Los Estados miembros, las autoridades de control, el Comité y la Comisión promoverán la creación de mecanismos de certificación en materia de protección de datos y de sellos y marcas de protección de datos a fin de demostrar el cumplimiento de lo dispuesto en el Reglamento en las operaciones de tratamiento de los responsables y los encargados.

El establecimiento de mecanismos de certificación y sellos de calidad, permite evaluar rápidamente el nivel de protección de una empresa.

El RGPD también hace hincapié en la rendición de cuentas eficaz al hablar de las siguientes medidas, entre otras:

- Registro de actividades: nueva obligación de documentación del tratamiento para los responsables o los encargados que deben llevar a cabo un registro de tas las actividades de tratamiento que realicen.
- Protección de datos desde el diseño: el responsable aplicará, tanto en el momento de determinar los medios de tratamiento como en el tratamiento mismo, las medidas técnicas y organizativas adecuadas para ofrecer las garantías necesarias y cumplir los requerimientos del Reglamento.
- Protección de datos por defecto: el responsable aplicará las medidas técnicas y organizativas adecuadas para garantizar que, por defecto, sólo se traten los datos personales necesarios para cada finalidad específica del tratamiento.
- Medidas de seguridad: el RGPD no estipula un listado de las medidas de seguridad a aplicar, sino que establece que el responsable sea quien decida qué medidas técnicas y organizativas son las adecuadas según el riesgo que conlleva el tratamiento.
- Evaluaciones de Impacto: cuando sea probable que un tratamiento, especialmente si se utilizan las nuevas tecnologías, por su naturaleza, alcance, contexto o finalidades, suponga un alto riesgo para los derechos y libertades de las personas físicas, el responsable debe realizar una evaluación del impacto.
- Autorización previa o consultas previas: si tras la evaluación de impacto se observa que el tratamiento previsto podría infringir el RGPD, el responsable debe hacer una consulta a la autoridad de control para conocer la manera correcta de proceder.
- DPD: es el encargado de informar y asesorar al responsable o al encargado y a los trabajadores sobre las obligaciones que impone la normativa, supervisar su cumplimiento, asesorar sobre la evaluación de impacto y cooperar con la autoridad de control, entre otras tareas.
- Notificación de violación de seguridad: si se produce una violación de la seguridad, el responsable debe notificarlo a la autoridad de control en un plazo máximo de 72 horas, y de ser el caso a los afectados.

MATERIAL COMPLEMENTARIO

- Guia de La AEPD "Guía de Privacidad desde el Diseño". Consulta la guía en este enlace.
- Guía de Protección de Datos por Defecto (AEPD). Consulta la guia en este enlace.
- Gestión del riesgo y evaluación de impacto en tratamientos de datos personales (AEPD). Consulta la guía en este enlace.
- Guía para la gestión y notificación de brechas de seguridad (AEPD). Consulta la guía en este enlace.
- Guía del Reglamento General de Protección de Datos para Responsables de Tratamiento (AEPD). Consulta la guía en este enlace.
- GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS DEL ARTÍCULO 29 publicó en 2010 el Dictamen 3/2010 sobre el principio de responsabilidad, WP 173, en el que explicaba su significado y alcance. Consulta el dictamen en este enlace.

NOTICIAS

- **Las empresas informativas y las agencias de noticias podrán negociar de manera independiente con las grandes tecnológicas como Google y Facebook una remuneración por la difusión de sus contenidos** en línea siempre que estas obtengan una autorización previa y el acuerdo entre las dos partes se haga con "buena fe contractual, diligencia debida, transparencia y respeto a las reglas de la libre competencia, excluyendo el abuso de posición de dominio en la negociación**"**. Consulta el artículo en **este enlace.**

- **La AEPD advierte que los registros de datos biométricos de las jornadas laborales son invasivos:** Los registros de jornada de carácter biométricos son muy invasivos y manejan demasiados datos personales, según la AEPD que en una reciente resolución, finalizada por pago voluntario, sanciona a Servicios Logísticos Martorell Siglo XXI con 20.000 euros por la implantación de dicho registro a su cliente automovilístico SEAT. Consulta el artículo en este enlace.

- **La AEPD aborda en su blog Anonimización y seudonimización (II): la privacidad diferencial.** En la búsqueda de un equilibrio entre la explotación legítima de la información y el respeto a los derechos individuales han surgido estrategias encaminadas a preservar la utilidad de los datos al tiempo que se respeta la privacidad de las personas. Una de ellas es la privacidad diferencial, que trata de establecer garantías de protección de datos desde el diseño mediante la implementación práctica de estrategias de abstracción de la información, así es como lo aborda la Agencia en este blog. Consulta el blog en este enlace.