CEU
Universidad
San Pablo

Caso 4. Comentarios a la Guía *4/2019 sobre el Articulo 25*

Máster Universitario de Protección de Datos. Curso 2018-2019

Salvador Gaitán Roca

COMENTARIOS AL DOCUMENTO

1. INTRODUCCIÓN.

Nos encontramos ante unas directrices acerca de la implementación por diseño o por defecto de la protección de datos, contemplada en el artículo 25 del RGPD:

Protección de datos desde el diseño y por defecto

1. Teniendo en cuenta el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas, como la seudonimización, concebidas para aplicar de forma efectiva los principios de protección de datos, como la minimización de datos, e integrar las garantías necesarias en el tratamiento, a fin de cumplir los requisitos del presente Reglamento y proteger los derechos de los interesados.

*2. **El responsable del tratamiento** aplicará las medidas técnicas y organizativas apropiadas con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento. Esta obligación se aplicará a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad. Tales medidas garantizarán en particular que, por defecto, los datos personales no sean accesibles, sin la intervención de la persona, a un número indeterminado de personas físicas.*

3. Podrá utilizarse un mecanismo de certificación aprobado con arreglo al artículo 42 como elemento que acredite el cumplimiento de las obligaciones establecidas en los apartados 1 y 2 del presente artículo.

Estas directrices están centradas en ayudar al responsable del tratamiento a llevar a cabo esta implementación, pero también pueden ser de ayuda para los proveedores de servicios tecnológicos. Resulta de capital importancia tener en cuenta esta guía habida cuenta de que (y como comentamos más adelante en este trabajo) no existe una suerte de medidas especificas a implementar, al contrario que ocurría anteriormente en nuestro país.

2. SOBRE LAS MEDIDAS TÉCNICAS Y ORGANIZATIVAS.

Cuando se hace alusión a que el responsable deberá implementar las medidas técnicas y organizativas que sean necesarias para asegurar la integridad del dato, no solo se hace referencia a medidas de corte mayoritariamente tecnológico o informático, sino también a medidas relativas a la formación del personal de la empresa (un ejemplo comentado en clase, asegurarse de que los empleados no pegan con un post-it en el monitor del ordenador sus credenciales).

Existe además una segunda línea de defensa que deberá implementarse con el fin de asegurarse de que ante una brecha de seguridad los datos no se vean comprometidos, a través de la anonimización de los mismos.

3. SOBRE LOS RESPONSABLES DEL TRATAMIENTO

Conviene destacar que el artículo 25 no establece medidas concretas a llevar a cabo, sino que permite al responsable adecuar la seguridad a las condiciones generales del dato protegido. Además, los responsables deberán de ser capaces de demostrar que llevaron a cabo las medidas necesarias para proteger el dato. Se recomienda así el uso de indicadores (que pueden ser cuantitativos o cualitativos) que demuestren la efectividad de las medidas en cuestión. A título de ejemplo: evaluaciones de resultado, informes de expertos, reducciones en el tiempo de respuesta ante sujetos que ejerzan sus derechos sobre sus datos…

4. EL CONCEPTO DE: “STATE OF THE ART”

Se trata de un concepto muy presente en la legislación europea, como por ejemplo en materia de medio ambiente. Este concepto que no tiene una traducción directa al castellano, pero que referencia a aquel producto o concepto que incluye las mas modernas ideas y los más avanzados procedimientos.

En el RGPD se hace referencia a esto tanto en el artículo 32 como en el 25, puesto que se obliga al responsable a tener en cuenta el progreso actual en tecnologías de seguridad informática, o en

formación de empleados, puesto que no solo se aplica a materias puramente técnicas, sino también organizacionales.

Es, por tanto, un concepto dinámico y no estático, puesto que depende del momento temporal en el que nos encontremos.

5. PROTECCIÓN POR DISEÑO: MOMENTO TEMPORAL.

Para que la protección sea establecida por diseño, esta debe efectuarse en el momento en el que se están planeando y diseñando los medios por los que se va a tratar el dato, es decir, cuando van a establecerse procedimientos como la recogida del dato, el procesamiento de éste, los protocolos que se han de seguir…

Los responsables han de ser capaces de demostrar que han tenido en consideración este principio.

6. LA PROTECCIÓN POR DEFECTO

La protección de datos por defecto hace referencia a la existencia de valores preconfigurados acerca del tratamiento y uso que se va a hacer de los datos recogidos. Por ejemplo, animar a una plataforma de redes sociales a configurar los parámetros del perfil de los usuarios en el entorno que más proteja la intimidad, limitando desde el primer momento la accesibilidad del perfil de los usuarios para que por defecto no sea accesible a un número indefinido de personas.

Sobre las medidas técnicas y organizativas aplica lo mismo que aplicaba en el punto 2 de este caso práctico, pero esta vez de forma específica en el principio de minimización del dato.

7. IMPLEMENTACIÓN DE LOS PRINCIPIOS DE LA PROTECCIÓN DE DATOS

Sobre esto, la guía menciona lo siguiente:

En primer lugar, el responsable ha de tener en cuenta estos principios en todo momento, y deberá seguir la guía comentada, que ilustra con ejemplos cada uno de estos principios. Estos ejemplos no hacen referencia a un principio de forma exclusiva, sino que a veces puede corresponderse o hacer referencia a varios principios.

Además, se incluye una lista de elementos clave para establecer un sistema de protección de datos por diseño y por defecto, como por ejemplo la no discriminación, la autonomía, o el respeto a los derechos y libertades individuales.

8. SOBRE EL CERTIFICADO DE LA PROTECCIÓN DEL DATO.

Añade la guía que el artículo 25.3 hace referencia a un certificado de la protección de datos por diseño: "*Podrá utilizarse un mecanismo de certificación aprobado con arreglo al artículo 42 como elemento que acredite el cumplimiento de las obligaciones establecidas en los apartados 1 y 2 del presente artículo.*"

Si un responsable cuenta con este certificado, las autoridades encargadas de la supervisión de la seguridad de los datos deben tenerlo en cuenta, puesto que implica una conformidad con el RGPD y en especial con la protección de datos por defecto y desde el diseño.

9. RÉGIMEN SANCIONADOR

Las autoridades anteriormente mencionadas podrán advertir al responsable o encargado del tratamiento, sancionarle u ordenarle que respete los derechos del sujeto cuyos datos se han tratado. Estas facultades vienen atribuidas a través del artículo 58.2 del Reglamento ("*cada autoridad de control dispondrá de todos los siguientes poderes correctivos indicados a continuación […]")*

La guía estudiada comenta que el nivel de consideración que el responsable o encargado a tenido para con la protección de datos desde el diseño o por defecto es un elemento clave a la hora de determinar la sanción impuesta, tal y como se especifica en el artículo 83.4

10. CONCLUSIONES Y RECOMENDACIONES

Se advierte que el adherirse correctamente a estas bases de planteamiento de un sistema de protección de datos desde el diseño y por defecto es de capital importancia en una sociedad cada vez más tecnológica. Además, a pesar de no aparecer de forma explícita en el artículo 25 del RGPD los proveedores de servicios tecnológicos deberán tener a bien considerar esta guía para desarrollar su actividad.

Por último, la guía establece una lista de recomendaciones a seguir por los responsables y encargados del tratamiento si lo que quieren es realizar una implementación efectiva de las ya mencionadas medidas técnicas y organizativas. A título de ejemplo, entre estas recomendaciones encontramos:

- Considerar la protección de datos desde el diseño y por defecto desde las primeras fases de elaboración del plan que el responsable o encargado va a seguir mientras trate datos de carácter personal.
- Los responsables y encargados deberán tener en cuenta las posibles sanciones economicas en las que pueden incurrir a la hora de considerar los costes de implementar unas medidas técnicas y organizativas correctas y eficaces.
- Los responsables y encargados del tratamiento deberán ser completamente transparentes ante los sujetos cuyos datos estén tratando, respetando así el principio de transparencia.