

Comentarios a la Guía 4/2019 acerca del artículo 25 del Reglamento (UE) 2016/679 relativo a la protección de las personas físicas en lo que respecta al tratamiento de y a la libre circulación de esos datos referido a la protección de datos desde el diseño y por defecto.

NOMBRE ALUMNA: Marcela Alejandra Román Rodríguez.

FECHA: 14 de enero de 2020.

- 1- La Guía establece recomendaciones para el cumplimiento de la obligación de protección de datos desde el diseño y por defecto del artículo 25 del Reglamento (UE) 2016/679 relativo a la protección de las personas físicas en lo que respecta al tratamiento de y a la libre circulación de esos datos (En adelante RGPD) y por tanto, va dirigido principalmente a los responsables del tratamiento de datos, puesto que este artículo se encuentra enmarcado en las obligaciones del responsable y del encargado. Es por ello, que será perentorio su conocimiento, aplicación práctica (que es lo que propone a través de ejemplos) y demostración en función del principio de responsabilidad activa. Sin embargo, la mayoría de las recomendaciones sugeridas al final del texto, va dirigida a los proveedores de tecnología, lo que debería tenerse en cuenta a la hora de considerar la aplicación del RGPD, puesto que también tienen un papel relevante en el cumplimiento de los principios que establece la regulación.
- 2- Se trata del desarrollo y análisis de un artículo de vital importancia, puesto que el art. 25 RGPD establece una obligación para el responsable que engloba de manera integrada los requisitos y derechos necesarios para su objeto en el tratamiento de datos y es justamente lo que se resalta a lo largo del mismo, ya que impone el cumplimiento de principios y derechos de los interesados aun antes del inicio del tratamiento, lo que le da un carácter de imposición continua y permanente. Es por ello que resulta interesante ver como se diseña a través del documento la obligación de cumplimiento del artículo, desde un punto de vista temporal.
- 3- No se limita el ámbito de las medidas prácticas y se recalca la no exigencia determinada de ellas, sino su indefinición en cuanto a su eficacia al momento de analizar en un tratamiento determinado, para la aplicación del principio de responsabilidad activa. Estas son de amplio espectro, en el sentido de que se mencionan de manera general varias de distinta complejidad de aplicación técnica y económica, lo que permitiría en teoría la aplicación de las mismas en

empresas pequeñas y también grandes, dando un amplio rango de elección de herramientas para la protección de datos personales durante el tratamiento.

- 4- La seudonimización se destaca como una medida de salvaguarda de los datos personales y para implementar una serie de principios, pero se sabe que no es la medida mas segura para la protección de datos. En realidad, para evitar el tratamiento de datos personales como la forma mas segura, quizás sería mejor recomendar la anonimización si es que el dato no requiere de posterior verificación o una recogida anónima establecida en el diseño del tratamiento, de manera tal de cumplir con el principio de minimización y finalidad¹, así como también con la temporalidad en el tratamiento de datos, evitando así incluso el ámbito de aplicación del RGPD, con todo el ahorro y beneficio económico de recursos que ello acarrea.
- 5- La efectividad se destaca como elemento nuclear del artículo, así como la necesidad de demostración de la implementación de las medidas de protección por diseño y por defecto. Como el art. 25 no establece medidas de manera particular, pero si la necesidad de demostración de las mismas en el número 3, podrían exponerse algunas medidas prácticas en ese sentido mas allá de la certificación, puesto que se enumeran en el Nº 16 matrices e instrumentos que parecen mas adecuados para la evaluación del riesgo de las medidas adoptadas (como son aquellas cuantitativas referidas a los niveles de riesgo, reducción de quejas, reducción de tiempos de respuestas, evaluaciones de desempeño) y que son instrumentos generalmente utilizados en grandes empresas que tratan grandes cantidades de datos personales. Algunas de ellas podrían ser la demostración de realización de cursos o capacitaciones para los trabajadores en cuanto a seguridad laboral, a la utilización de herramientas de seguridad, e incluso hábitos en los puestos de trabajo en cuanto a los equipos en que se almacenan los datos personales tratados, que pueden implicar riesgos e incumplimiento del principio de confidencialidad.
- 6- Se destaca a lo largo de todo el documento la importancia de la evaluación de riesgos de incumplimiento, como una herramienta importante al momento de prever la efectividad de una medida tomada en el ámbito del art. 25 del RGPD, ya que permite determinar antes del tratamiento de datos, el grado de cumplimiento de la protección desde el diseño y por defecto, que es el objeto principal del RGPD. Esta regulación para la protección de datos personales se centra en la evitación de infracciones en el tratamiento de ellos, siendo el art. 25

¹ Pseudonymisation is also addressed to clarify some pitfalls and misconceptions: pseudonymisation is not a method of anonymisation. It merely reduces the linkability of a dataset with the original identity of a data subject, and is accordingly a useful security measure. The Opinion concludes that anonymisation techniques can provide privacy guarantees and may be used to generate efficient anonymisation processes, but only if their application is engineered appropriately – which means that the prerequisites (context) and the objective(s) of the anonymisation process must be clearly set out in order to achieve the targeted anonymisation while producing some useful data. The optimal solution should be decided on a case-by-case basis, possibly by using a combination of different techniques, while taking into account the practical recommendations developed in this Opinion. Disponible en web: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf

Máster en Protección de Datos Personales, Transparencia y Acceso a la Información.

una muestra destacable, puesto que impone obligaciones aun antes de recoger datos personales. Sin embargo, el uso de la evaluación de riesgos no es obligatoria en todos los casos como señala el artículo 35 del RGPD, lo que parece adecuado debido a los costos económicos que pueden resultar desproporcionados para micro empresas y autónomos². Es por ello, que establecer también ejemplos de medidas de cumplimiento y que refuercen el principio de responsabilidad proactivo distintos, serían de ayuda para este tipo de emprendimientos.

- 7- Se dan recomendaciones específicas a los encargados de los objetivos técnicos en la protección de datos, (como son los desarrolladores de tecnologías, encargados de software). Siendo que el tratamiento de datos se desarrolla en su gran mayoría por sujetos técnicos, (como señala por ejemplo en su guía noruega³ cuando se refiere el la protección desde el diseño y por defecto), quizás sería interesante incluir algún tipo de regulación, sanción o como criterio de ajuste en la aplicación de multas, para aquellos casos en que el diseño tecnológico favorezca la aplicación de este principio, fuera de la certificación que no siempre es uniforme entre distintos países miembros y puede dar lugar a criterios objetivamente desiguales en cuanto al cumplimiento.
- 8- El sistema de ejemplos a través de los principios usado en esta guía, así como en otras del grupo de trabajo del artículo 29, es muy destacable puesto que pone en perspectiva el análisis teórico que también gracias a los elementos clave indicados clarifica mucho la orientación con la que ha de comprenderse la norma en análisis. Así como también, las referencias a documentos emanados de entidades nacionales de países miembros que también están implementando y orientando respecto de la aplicación de la regulación de protección de datos personales. Sería deseable que estos ejemplos fueran más específicos en cuanto a las mejores técnicas y estructura metodológica a utilizarse para el cumplimiento de los principios y con mayor detalle de las medidas concretas que se consideran como efectivas, como por ejemplo se hace en la “Guía de Privacidad desde el Diseño” de la Agencia Española de Protección de Datos⁴.
- 9- Ya que las medidas de protección de la privacidad desde el diseño y por defecto se exige sin considerar el costo económico podría establecer alguna ayuda o incentivo a pequeñas empresas que tratan datos de manera masiva o sensibles y que se ven obligados a efectuar evaluaciones de riesgo y tomar otras medidas tecnológicas de alto costo para incentivar la aplicación del RGPD.
- 10- Como ya se mencionó, se trata de una Guía que desde el punto de vista jurídico integra los principios de la norma de manera clara y completa, con aportes muy

² En el caso de España se ha publicado por la Agencia Española de Protección de Datos la “Listas de tipos de tratamientos de datos que requieren evaluación de impacto relativa a protección de datos (art. 35.4). Disponible en web: <https://www.aepd.es/sites/default/files/2019-09/listas-dpia-es-35-4.pdf>

³ Disponible en web en: <https://www.datatilsynet.no/en/about-privacy/virksomhetenes-plikter/innebygd-personvern/data-protection-by-design-and-by-default/?id=7729&id=7729>

⁴ Disponible en web: <https://www.aepd.es/sites/default/files/2019-11/guia-privacidad-desde-diseno.pdf>

interesantes de desarrollo normativo, especialmente en el punto 2, lo que para un jurista es muy deseable. Pero deja un poco de lado las consideraciones prácticas que requiere un responsable del tratamiento de datos, más allá del ámbito regulatorio. Lo opuesto ha de suceder con delegados de protección de datos que no sean juristas, por cuanto la guía contiene mucha información orientada específicamente a juristas, pero no estructura práctica para el cumplimiento del artículo. Se extrañan medidas concretas y específicas, u orientaciones metodológicas paso a paso en orden a centrar el desarrollo de este importante artículo a la eficacia en su aplicación por parte de los responsables del tratamiento, que es a quienes va dirigido el objeto de este principio esencial y de intrínseca incorporación, a toda la regulación del RGPD.