Guidelines 4/2019 on Article 25 Data Protection by Design and by Default

Observaciones elaboradas por Alicia Piñar Real
Abogada
España

El Comité Europeo de Protección de Datos ha elaborado el borrador de "Directrices sobre el Artículo 25 del RGPD – Protección de Datos desde el diseño y por defecto", borrador que se encuentra desde el 20 de noviembre de 2019 sometido a consulta pública. La fecha límite para el envío de las observaciones finaliza el 16 de enero de 2020 y las mismas deben ser enviadas a través del formulario que aparece en la página web del Comité https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2019/guidelines-42019-article-25-data-protection-design_es

Como estudiante del Máster en Protección de Datos, Transparencia y Acceso a la Información de la Universidad CEU San Pablo (España) y en la confianza de que puedan resultar de interés a lo largo de la elaboración definitiva de las Directrices, dentro del plazo establecido para ello se remiten los siguientes comentarios.

PREELIMINAR:

El objetivo de las Directrices es, tal y como se señala en su resumen, ofrecer una orientación general sobre la obligación de protección de datos desde el diseño y por defecto establecida en el Art. 25 del RGPD.

OBSERVACIONES:

PRIMERA.- La elaboración de las presentes Directrices resulta oportuna y necesaria ya que el Art. 25 RGPD es una de las grandes novedades del Reglamento y recae sobre los responsables del tratamiento el poder demostrar la eficacia de las medidas aplicadas. Así pues, que los responsables puedan contar con una serie de Directrices que les ayuden a entender cumplido su deber de responsabilidad proactiva es, sin duda, de gran utilidad.

SEGUNDA.- La segunda de las observaciones se refiere al título del documento. Parece más oportuno cambiar el título a "Directrices sobre la protección de datos desde el diseño y por defecto" (evitando la palabra "principio" ya que no se encuentra entre los principios – Arts. 5 a 11 RGPD– sino entre las obligaciones del responsable). Y esto porque, si bien es cierto que el Artículo 25 del Reglamento es el principal sobre el

asunto, la regulación debe verse desde el conjunto sin olvidar los Considerandos 39, 78 y 108 y los artículos como el 47.

TERCERA.- Enlazando con lo anterior, en las Directrices no se habla del Artículo 47, relativo a las normas corporativas vinculantes, y la obligación de especificar en las mismas la aplicación, entre otros, de la protección de datos desde el diseño y por defecto.

CUARTA.- Ya que la protección de datos desde el diseño y por defecto tiene como objetivo final proteger al titular de los datos mediante la imposición de una obligación al responsable del tratamiento, se podría incidir más en este aspecto para que la lectura de las recomendaciones se hiciera desde una perspectiva de garantía de derechos más que de obligaciones a cumplir.

QUINTA.- La Agencia Española de Protección de Datos publicó en octubre de 2019 su Guía de Privacidad desde el Diseño https://www.aepd.es/sites/default/files/2019-11/guia-privacidad-desde-diseno.pdf

Esta Guía dedica 13 páginas, con columnas con correspondencias, a un Anexo sobre la Selección de patrones de diseño de la privacidad. La primera columna indica el nombre del patrón de diseño (por ejemplo: Auditorías), la segunda el objetivo y la finalidad (ejemplo: Realizar auditorías periódicas para examinar la efectividad de los mecanismos de cumplimiento) y la tercera la/s estrategia/s a la/s que da soporte (en el ejemplo, demostrar).

Se echa en falta en el documento del Comité Europeo un anexo de este tipo que ofrece multitud de patrones que acercan a la práctica los tecnicismos y requerimientos de las Directrices.

SEXTA.- Igualmente, sería interesante que las Directrices incluyeran los Principios Fundacionales de la Privacidad desde el Diseño definidos por Ann Cavoukian https://www.iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf Su lectura es sencilla y están redactados en un lenguaje comprensible y accesible.

SÉPTIMA.- Un aspecto que podría ser añadido aportando una visión práctica de la cuestión sería un apartado sobre ingeniería de privacidad, también presente en la Guía de la AEPD, traduciendo los principios de privacidad desde el diseño en medidas concretas, ya sea desde su concepción ya sea durante su desarrollo. Efectivamente, los llamados PETS (Privacy Enhancing Technologies) son, en palabras de la Agencia, "un conjunto organizado y coherente de soluciones TIC que reducen los riesgos que afectan a la privacidad, implementando las estrategias y patrones definidos

anteriormente". Tras clasificarlos, la Guía incluye un catálogo de PETS detallando el portal, la organización, la url y la descripción. Contar con un apartado de este tipo enriquecería el documento de Directrices.

OCTAVA.- El apartado 5, "Aplicación del artículo 25 y consecuencias" resulta sorprendentemente corto, limitándose a enumerar los preceptos aplicables pero sin hacer ninguna aportación reseñable.

NOVENA.- Dentro del apartado de las recomendaciones, el cuarto punto habla de que "*Los proveedores de tecnología deben desempeñar un papel activo para garantizar el cumplimiento de los criterios del "estado actual de la técnica" y notificar a los controladores cualquier cambio (…) Los responsables deben incluir este requisito como una cláusula contractual para asegurarse de que se mantienen actualizados*". Esta recomendación, aunque se entiende positiva y compartimos su finalidad, puede resultar de difícil cumplimiento en los casos en los que el proveedor de tecnología vende un servicio, se paga la contraprestación y la relación termina. El proveedor de tecnología puede entender que no está obligado a realizar ninguna acción una vez que haya finalizado la relación contractual. Por eso, el responsable deberá estar atento ya que en los casos en los que por ejemplo se esté contratando un servicio en SaaS incluir esta previsión contractual será más sencillo pero en los casos en los que, por ejemplo, se contrate un desarrollo que posteriormente será gestionado dentro de la empresa del propio responsable, desvinculándose el proveedor, una cláusula que incluya posibles responsabilidades futuras al proveedor y una obligación activa de notificación de novedades, cuando ya la relación ha finalizado, podría no ser aceptada por el proveedor. Para incentivar la aceptación, podría proponerse el pago de alguna cantidad por cada notificación de novedades que hiciera el proveedor y que cumplieran una serie de requisitos pactados (*win – win*)

No olvidemos que la obligación es del responsable y será este el que deberá estar atento al estado del arte sin poder traspasar completamente esta obligación al proveedor de tecnología.

DÉCIMA.- Finalmente, y como cuestión de edición del texto, me resulta confuso que los apartados que se incluyen en los epígrafes de numeración X. X. X. no lleven numeración. Por ejemplo, en el apartado *2.1.3 Elements to be taken into account*, la numeración de los elementos simplemente aparece enunciada entre comillas y empezando incluso con minúscula: "*state of the art*", "*cost of implementation*", etc. Sería más correcto que fuera *a) State of the art, b) Cost of implementation*, etc.

Madrid, a 13 de enero de 2020