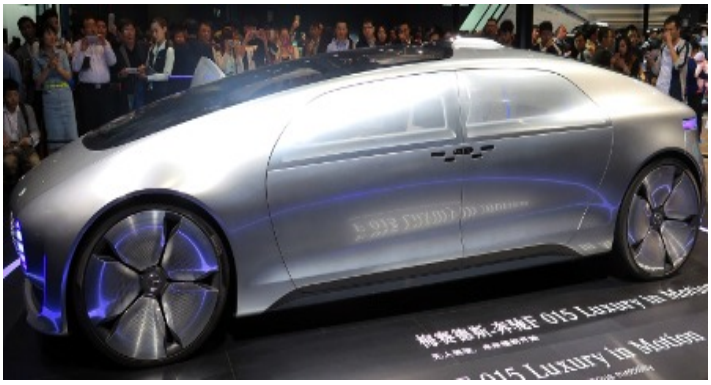
EUROPA PRESENTA SU NUEVO REGLAMENTO

Con ocasión del lanzamiento del nuevo prototipo europeo de protección de datos, los rumores y la espera han terminado. Nos subimos en él para probarlo y contaros las sensaciones.

Descubrimos y probamos el nuevo reglamento de protección de datos europeo. Análisis de comportamiento y perspectiva en la versión full-time. Ventajas e inconvenientes. Perspectivas de aplicación del reglamento.



Como el típico artículo especializado de motor y aprovechando el reciente Salón Legislativo Europeo celebrado el pasado 4 de mayo, en el cual se presentó, a través del DOCE, el gran lanzamiento del nuevo reglamento de protección de datos, el cual ya se encuentra disponible en su gama comercial de oferta de lanzamiento en dos tipo de versiones, full-equipe para grandes empresas y basic para pymes, con equipamientos de serie en virtud de dichas versiones, pudiendo los usuarios disponer del mismo en los próximos dos años con versiones ampliadas y equipamientos extras que irán conformando su versión definitiva.

Lo primero que resalta del Reglamento es la intención de presentar dos versiones diferenciadas, puestas de manifiesto en el considerando (13)[1], al efectuar una referencia de intenciones -minimizar las obligaciones y deberes- a microempresas y Pymes, pero no más lejos de la realidad, puesto que si nos acomodamos en aquél, la versión exclusivamente será full-equipe, salvo que la Comisión considere efectuar versiones con equipamiento basic a través de los actos delegados[2]. Por tanto, a fecha presente, solamente existe la versión full-time con equipamiento de serie indistintamente del destinatario, puesto que el Reglamento no define, ni cualitativa ni cuantitativamente, lo que considera *"tratamiento no ocasional"* ni *"observación habitual y sistemática"*, destacando entre su equipamiento: el registro de actividades de tratamiento, designación de delegado de protección de datos, transparencia, sellos y marcas de protección de datos, y otros adicionales. Así mismo, al menos, el reglamento extiende el ámbito de aplicación a empresas fuera de la Unión Europea[3] -elaboración de perfiles y ofrecimiento bienes/servicios- y establece el concepto de "seudonimización."

Al margen de la versión, la primera impresión es buena, con una estética que pretende acoplarse a los nuevos tiempos, dándole un "aire" mejorado de la antigua versión -Directiva 95/46- pero que no alcanza a cumplir las perspectivas que del mismo se esperaba. Carece y se echa de menos múltiples definiciones, tales como: tratamiento a gran escala, verificación, mercadotecnia, información adicional, utilizando términos básicos como "información", "dato" y "dato de carácter personal" que, en muchos casos, son mezclados provocando confusión.

El Reglamento cuenta con una capacidad de almacenaje que lo convierte en el puntero del sector, ya que todo tiene cabida a través del sistema "interés público" o "misión de interés público", concepto indeterminado, que puede ser la "tapadera" o "embudo" en el que amparar cualquier situación afecta al tratamiento de datos personales, esperando que legislativamente, el requisito de necesidad y proporcionalidad para calificar el tratamiento o misión de interés público, sea suficiente para mantener la calificación de puntero en cuanto a capacidad de carga.

En cuanto al consumo, elevado y excesivo, en todas sus variantes, tanto para el sector público en su ámbito legislativo -el nuevo gobierno tendrá mucho actividad legislativa al respecto-; como en el sector privado, en su ámbito organizativo y técnico, repercutiendo en un sobrecoste, con la finalidad aparente de dotar de mayor seguridad al tratamiento de datos personales.

En cuanto al sistema de seguridad, aparentemente potente, destacando la comunicación de brechas de seguridad y dotando de sistema Isofix para menores, si bien bajo el complejo sistema de verificación, no autenticación, y su compleja ingeniería para acomodarlo, efectuando salvedad para lo que se denomina *"contexto de servicios preventivos o de asesoramiento ofrecido directamente a los niños."* Al presente sistema de seguridad, ha de sumarse, el sistema de transparencia que, aparentemente, obligará a los responsables y encargados de tratamiento a disponer de información respecto al sistema de protección, tanto legal, organizativo y técnico -otro enlace más en Páginas Web.-

Una novedad interesante es que la versión del nuevo reglamento pretende ser una copia del sistema establecido para el cumplimiento de la normativa de prevención del blanqueo de capitales y financiación del terrorismo -LBCFT-, en cuanto al nombramiento de un intermediado que sea el contacto con la autoridad de control -DPO-, asesorar en el ámbito propio de aplicación de la normativa, disponer de la política interna -organizativa y técnica- respecto al tratamiento, lo que provoca eliminar o acoplar el denominado *"documento de seguridad"* y *"registros de ficheros"*, junto a los Impactos de Evaluación así como los Privacy-Design. En síntesis, idéntica similitud y, previsiblemente, los DPO al igual que los intermediarios con el SEPBLAC deberán darse de alta en el sistema de la Agencia de Protección de Datos, lo que implica un desarrollo legislativo respecto al presente ámbito.

La nueva versión dará lugar a la proliferación de talleres de adecuación "piratas", más aún con la exigencia o recomendación sibilina de certificaciones, códigos de conducta, marcas y sellos de protección de datos, unido al poder conferido a entidades, organizaciones o asociaciones sin ánimos de lucro -FACUA, OCU, u otras que se constituyan con el objeto social de defensa de intereses en protección de datos.- Visto, igualmente, el lado positivo, al menos, se reconoce la práctica de abogados en dicha materia como pilar para ostentar la condición de DPO.

Por extensión y porque se necesita más tiempo para probar en diferentes terrenos el nuevo reglamento, un simple inciso respecto a las responsabilidades y, especialmente, a la posibilidad de los interesados de acudir a la vía jurisdiccional directamente en reclamación de daños y perjuicios, lo que puede suponer que el interesado no reclame directamente por una posible vulneración en el tratamiento de datos personales, sino que acuda a la vía jurisdiccional, tal vez, basándose como criterio objetivo en la multa sancionadora establecida en el propio reglamento, convirtiéndose tal vez en una resolución amistosa inter-partes (responsable vs interesado) que, en un determinado momento, pudiere compensar la sanción máxima entre 20 M € hasta un 4% de volumen de negocio. De igual forma, la posibilidad de sancionar penalmente, tendrá repercusión en los tan de moda Compliance Penal. Para concluir, solamente, insertar la curiosidad, del mecanismo de resolución amistosa entre el responsable y la autoridad de control establecida en el considerando (131)[4].

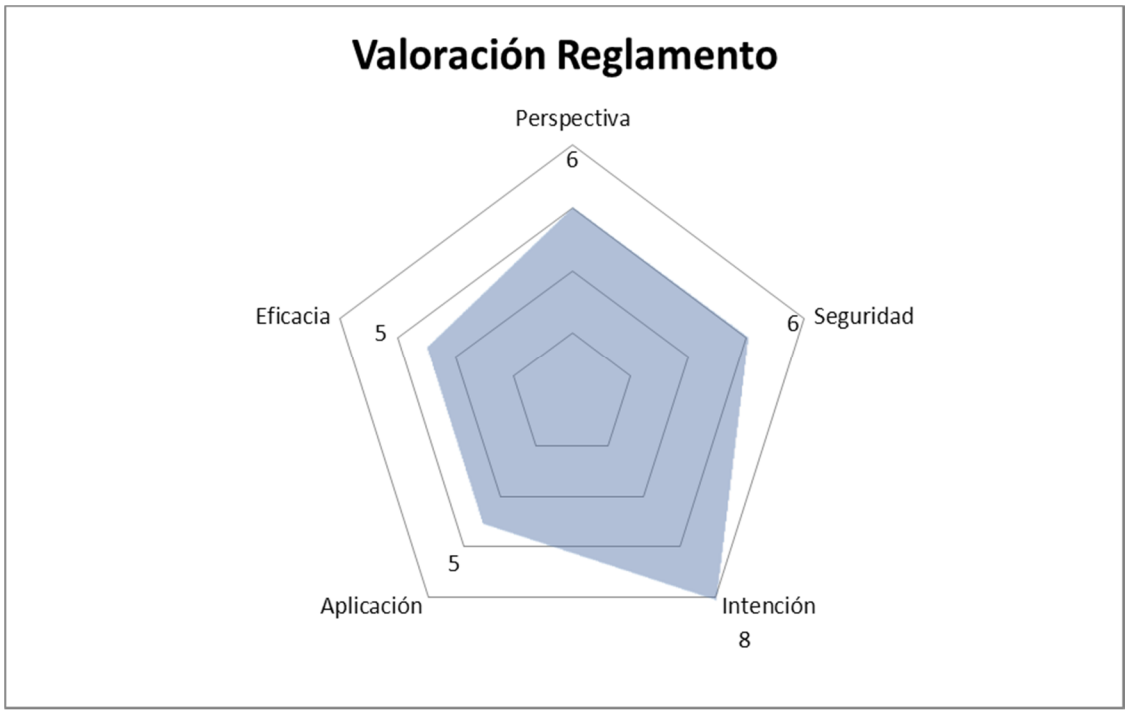
Ventajas

- Intención de dotar de un nuevo diseño y seguridad el tratamiento de datos personales.
- Aplicación fuera de la Unión.
- Reconocimiento de expertos o abogados especializados en la materia.
- Eliminación de trámites administrativos y similitud al sistema regulado para la prevención del blanqueo de capitales.

Inconvenientes

- Múltiples extras, complejos y que precisan de una mejor configuración, especialmente, para microempresas y PYMES.
- Consumo excesivo, legislativo, económico y de recursos humanos.
- Posibilidad de aparición de nuevos servicios similares al actual coste cero de adecuación
- Posible colapso del orden jurisdiccional por reclamaciones de daños y perjuicios.

La puntuación media que obtiene el reglamento tras efectuar una prueba mínima de kilometraje es de 6, debiendo ajustar dicha puntuación con el transcurso del tiempo, una vez se vaya configurando para su transposición a nivel estatal el articulado contenido en el mismo.



Efrén Santos Pascual
Socio - Abogado TIC
ICEF Consultores
@efrensantos_tic

[1] *"[…] Con objeto de tener en cuenta la situación específica de las microempresas y las pequeñas y medianas empresas, el presente Reglamento incluye una serie de excepciones en materia de llevanza de registros para organizaciones con menos de 250 empleados […]"*

[2] *Considerando (167) A fin de garantizar condiciones uniformes de ejecución del presente Reglamento, deben conferirse a la Comisión competencias de ejecución cuando así lo establezca el presente Reglamento. Dichas competencias deben ejercerse de conformidad con el Reglamento (UE) n.º 182/2011 del Parlamento Europeo y del Consejo. En este contexto, la Comisión debe considerar la adopción de medidas específicas para las microempresas y las pequeñas y medianas empresas.*

[3] Considerando (23) y (24), destacando que *"[…] el tratamiento de datos personales de interesados que residen en la Unión por un responsable o un encargado no establecido en la Unión debe regirse por el presente Reglamento si las actividades de tratamiento se refieren a la oferta de bienes o servicios a dichos interesados, independientemente de que medie pago […] debe determinarse si es evidente que el responsable o el encargado proyecta ofrecer servicios a interesados en uno o varios de los Estados miembros de la Unión. Si bien la mera accesibilidad del sitio web del responsable o encargado o de un intermediario en la Unión, de una dirección de correo electrónico u otros datos de contacto, o el uso de una lengua generalmente utilizada en el tercer país donde resida el responsable del tratamiento, no basta para determinar dicha intención, hay factores, como el uso de una lengua o una moneda utilizada generalmente en uno o varios Estados miembros con la posibilidad de encargar bienes y servicios en esa otra lengua, o la mención de clientes o usuarios que residen en la Unión, que pueden revelar que el responsable del tratamiento proyecta ofrecer bienes o servicios a interesados en la Unión."*

[4] *"En casos en los que otra autoridad de control deba actuar como autoridad de control principal para las actividades de tratamiento del responsable o del encargado pero el objeto concreto de una reclamación o la posible infracción afecta únicamente a las actividades de tratamiento del responsable o del encargado en el Estado miembro en el que se haya presentado la reclamación o detectado la posible infracción y el asunto no afecta sustancialmente ni es probable que afecte sustancialmente a interesados de otros Estados miembros, la autoridad de control que reciba una reclamación o que*

detecte situaciones que conlleven posibles infracciones del presente Reglamento o reciba de otra manera información sobre estas debe tratar de llegar a un arreglo amistoso con el responsable del tratamiento y, si no prospera, ejercer todos sus poderes [...]"