MOORE

LEGAL Y COMPLIANCE

CAMBIOS EN LA LEY DE PREVENCIÓN DEL BLANQUEO DE CAPITALES Y DE LA FINANCIACIÓN DEL TERRORISMO

La Ley 18/2022, de 28 de septiembre, de creación y crecimiento de empresas, publicada en el BOE el pasado 29 de septiembre, reforma la Ley 10/2010 de prevención del blanqueo de capitales y de la financiación del terrorismo en su disposición final segunda.

Se incorporan ciertas modificaciones relevantes ya recogidas en las últimas directivas europeas que no habían sido implementadas por nuestro ordenamiento. Incluye también previsiones enfocadas en el área de protección de datos de carácter personal y sus implicaciones en materia de PBC/FT.

Se modifica el **apartado 3 del artículo 2** de la Ley 10/2010 incluyendo entre los supuestos que podrían quedar **excluidos de la consideración de sujeto obligado las entidades de dinero electrónico, entidades de pago** y personas físicas y jurídicas referidas en el Real Decreto-ley 19/2018, de 23 de noviembre, de servicios de pago y otras medidas urgentes en materia financiera, **siempre que se pueda acreditar un escaso riesgo de blanqueo de capitales o de financiación del terrorismo**.

Se modifica la letra a) del apartado 1 del artículo 12 de la ley (**relaciones de negocio y operaciones no presenciales**) aclarando que en todos aquellos casos en que la **firma electrónica** utilizada no reuniese los requisitos de la firma electrónica cualificada seguirá siendo preceptiva la obtención, en el plazo de un mes desde que se inicia la relación de negocio, de una copia del documento de identificación. Es decir, aunque se acepta, en la identificación no presencial, la utilización de firma electrónica no cualificada, esta firma electrónica no eximirá de la obtención de copia de documento de identificación.

Se permite que los sujetos obligados que pertenezcan a la misma categoría (entidades de créditos, joyerías, aseguradoras...) puedan crear **sistemas comunes de información, almacenamiento y documentación recopilada**, para el cumplimiento de las obligaciones de diligencia debida establecidas en la Ley 10/2010. El mantenimiento de estos sistemas podrá encomendarse a un tercero, aun cuando no tenga la condición de sujeto obligado. Los datos obtenidos como consecuencia del acceso al sistema únicamente podrán ser empleados para el cumplimiento por los de las obligaciones de diligencia debida. Los sujetos obligados solo podrán acceder a la información facilitada por otro sujeto obligado en los supuestos en que la persona a la que se refieran los datos sea su cliente. Los datos serán facilitados al sistema por los órganos de control interno. Estos órganos canalizarán asimismo las solicitudes de acceso a los datos contenidos en el sistema.

Estos sujetos obligados tendrán la condición de corresponsables del tratamiento de los datos de este sistema y, por tanto, adquirirán nuevas obligaciones, entre otras: (i) la necesidad de comunicar su creación a la Comisión de Prevención del Blanqueo, (ii) informar a los interesados acerca de la comunicación de los datos al sistema, en su caso, o (iii) responder las solicitudes de ejercicios de derechos.

En materia de **protección de datos**:

Como principales cambios, encontramos el ajuste de los antiguos artículos de la LOPD 15/1999 a los correspondientes del RGPD, manteniendo algunos de los aspectos que ya se regulaban, como son;

i. la no necesidad de consentimiento,
ii. la exención del deber de informar del tratamiento de los datos para este fin y,
iii. la no procedencia de la atención de los ejercicios de derechos por parte de los interesados respecto de la información referida a operaciones sospechosas que se trasladan al Sepblac.

Como novedades principales en esta área, se pueden destacar:

La necesidad para los sujetos obligados de realizar una

EIPD (Evaluación de Impacto en la Protección de Datos) con el objetivo de adoptar las medidas técnicas y organizativas para garantizar la integridad, confidencialidad y disponibilidad de los datos personales. Dichas medidas deberán en todo caso garantizar la trazabilidad de los accesos y comunicaciones de los datos. El tratamiento lo deberán llevar únicamente a cabo los órganos de control interno.

De igual manera, los sujetos obligados o quienes desarrollen los sistemas que sirvan de soporte al intercambio de información a través de sistemas comunes de información deberán realizar una evaluación de impacto en la protección de datos de los citados tratamientos a fin de adoptar medidas técnicas y organizativas reforzadas para garantizar la integridad, confidencialidad y disponibilidad de los datos personales. Se aplicarán a estos ficheros las medidas de seguridad y control reforzadas.