ADAPTACIÓN AL REGLAMENTO EUROPEO DE PROTECCIÓN DE DATOS (RGPD)

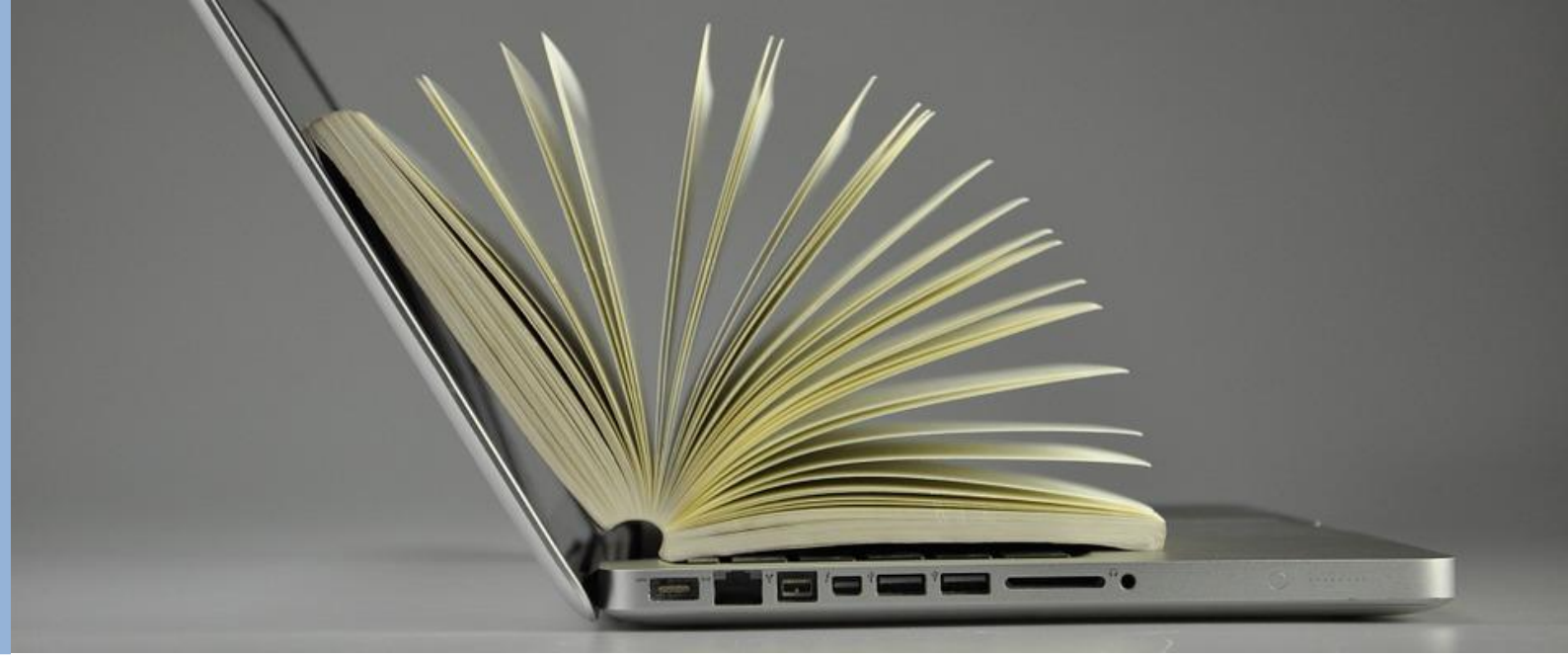
MARIMÓN
ABOGADOS

El nuevo Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (en adelante RGPD), entró en vigor el pasado 25 de mayo de 2016 y resultará de plena aplicación el próximo 25 de mayo del 2018.

Recientemente se ha presentado ante el Consejo de Ministros el anteproyecto de reforma de la Ley Orgánica de Protección de Datos con el fin de adaptar las disposiciones nacionales al nuevo marco europeo. Entre las novedades que incorpora el Anteproyecto está la reducción de la edad en la que los menores pueden consentir el tratamiento de sus datos que, a partir de ahora, se fija en los 13 años. Entre los cambios también hay novedades en relación con la regulación del tratamiento de datos de personas fallecidas.

Con este nuevo escenario normativo se pretende fortalecer la responsabilidad de las organizaciones que deberán garantizar el cumplimiento de las obligaciones en materia de protección de datos debiendo, asimismo, ser capaces de demostrar el cumplimiento documentando sus tratamientos. Las empresas disponen actualmente de un plazo de poco más de seis meses para llevar a cabo todas las actuaciones necesarias para adaptarse al nuevo marco legal.

Las empresas deberán realizar una serie de modificaciones antes del 25 de mayo de 2018 con el fin de adaptarse al nuevo Reglamento.



PRINCIPALES ACTUACIONES A LLEVAR A CABO

FASE 1.- Designar un Delegado de Protección de Datos

FASE 2.- Registrar las actividades de tratamiento

FASE 3.- Analizar los riesgos

FASE 4.- Realizar Evaluaciones de Impacto

FASE 5.- Revisar procesos internos

FASE 6.- Adaptar la documentación existente

FASE 7.- Documentar el cumplimiento

FASE 1.- DESIGNAR UN DELEGADO DE PROTECCIÓN DE DATOS

Para una adecuada gestión y coordinación de los datos personales de la organización, en determinadas ocasiones puede resultar necesaria la incorporación de la figura del Delegado de Protección de Datos (DPO). El DPO tiene como objetivos la información, la supervisión del cumplimiento, el asesoramiento y la cooperación respecto del cumplimiento de la normativa de protección de datos. Cabe recordar que la incorporación de un DPO antes de mayo de 2018 puede ofrecer a la organización una ventaja inicial significativa.

Las organizaciones deben incorporar un DPO obligatoriamente si se encuentran en alguno de los siguientes supuestos:

- Se trata de organizaciones públicas;
- Entidades que requieran monitorización periódica y sistemática de datos de personas a gran escala;
- Entidades cuya actividad principal consiste en el tratamiento de categorías especiales de datos;
- Cuando un país miembro o la Unión Europea lo impongan.

En determinadas ocasiones, incluso cuando la organización no esté obligada formalmente a designar esta figura, en empresas de cierto tamaño puede ser recomendable disponer de un DPO en aras de mejorar el cumplimiento de la normativa de protección de datos y minimizar los riesgos derivados del tratamiento. También es frecuente que los grupos de sociedades tengan criterios unificados para todas sus filiales independientemente de su tamaño.

Según el anteproyecto de ley española, podrían considerarse incluidos en estos criterios, entre otros:

- Entidades aseguradoras y reaseguradoras.
- Distribuidores y comercializadores de energía eléctrica o gas natural.
- Entidades responsables de sistemas de información crediticia.
- Entidades que desarrollen actividades de publicidad que impliquen análisis de preferencias o elaboración de perfiles.
- Centros sanitarios.
- Centros docentes que ofrezcan enseñanzas regladas, universidades.
- Colegios profesionales.
- Entidades dedicadas al juego *on line.*

FASE 2.- REGISTRAR LAS ACTIVIDADES DE TRATAMIENTO

Para medir eficazmente el impacto de la normativa europea sobre protección de datos en la empresa, hay que empezar por identificar con precisión los tratamientos y flujos de datos que la compañía lleva a cabo.

La entrada en vigor del RGPD implica la obligación de llevar a cabo un registro de actividades de tratamiento. Por ello, las empresas deben mantener un registro interno que disponga de información detallada sobre los tratamientos de datos que realicen, y el grado de cumplimiento de la normativa. Esta información deberá ser puesta a disposición de la Autoridad de control cuando sea requerida.

Por tanto, antes del mes de mayo de 2018, las empresas ya sean responsables o encargadas del tratamiento, deberán elaborar dicho registro interno con el fin de identificar y describir los tratamientos de datos llevados a cabo en el seno de la organización. Ello permitirá, además de cumplir con la normativa, poder disponer de un control efectivo sobre los datos personales tratados, así como detectar con mayor facilidad los posibles riesgos que existan durante el tratamiento.

FASE 3.- ANALIZAR LOS RIESGOS

Una vez realizado el registro de actividades de tratamiento, las organizaciones deben identificar las acciones que deben llevar a cabo para mitigar o, en su defecto, minimizar los riesgos detectados, con el fin de adaptarse a las obligaciones actuales y futuras en materia de protección de datos. Entre las acciones a realizar, deben priorizarse aquellas sobre tratamientos que conlleven un mayor riesgo de lesionar derechos y libertades de los interesados.

Esta priorización debe ser llevada con rigor y deben establecerse criterios en función de la sensibilidad de los datos, del ámbito en que se produce el tratamiento y del volumen de los datos tratados.

Durante el análisis de riesgos, para mitigar o, en su defecto, minimizar los riesgos, deberán adoptarse determinadas medidas de seguridad tanto técnicas como organizativas que eviten la pérdida de información, la destrucción involuntaria de datos o el acceso de un tercero no autorizado, y que a su vez garanticen la integridad, la disponibilidad y la inalterabilidad de los datos tratados.

FASE 4.- REALIZAR EVALUACIONES DE IMPACTO

En el caso de que se detecte que alguno de los tratamientos de datos personales llevados a cabo genera un alto riesgo para los derechos y libertades de los interesados, se debe elaborar una **evaluación de impacto** relativa a la protección de datos (en inglés, sus siglas PIA) para cada uno de ellos.

¿Cuándo se debe implementar la Evaluación de Impacto (PIA)?

- Antes de realizar cualquier tratamiento con un elevado riesgo de lesionar derechos y libertades de determinadas personas.

¿En qué escenarios debe elaborarse una Evaluación de Impacto (PIA)?

- En tratamientos que impliquen una *"evaluación sistemática y exhaustiva de aspectos personales de personas físicas"*;
- En tratamientos a gran escala de datos sensibles;
- En la observación sistemática a gran escala de una zona de acceso público.

Aún así, en determinados casos en los que no exista la necesidad de llevar a cabo la Evaluación de Impacto, puede resultar recomendable elaborarla, dado que es una herramienta útil para ayudar al responsable de tratamiento a tener un mayor control sobre el tratamiento en cuestión.

La Evaluación de Impacto es un instrumento esencial que sirve para aplicar el principio de responsabilidad proactiva (*accountability*). Así no sólo se facilita el cumplimiento de la norma, sino que además permite acreditar dicho cumplimiento.

El resultado final de una Evaluación de Impacto es un informe que recoge las características del tratamiento evaluado y las decisiones tomadas para mitigar o minimizar los riesgos. Ello se realiza a partir de la identificación, análisis, valoración y tratamiento (gestión de riesgos), y una vez analizadas cuestiones como el interés legítimo (en su caso) o la necesidad y la proporcionalidad de las operaciones de tratamiento.

FASE 5.- REVISAR PROCESOS INTERNOS

Para garantizar un alto nivel de protección de los datos personales, las organizaciones deben implementar procedimientos internos que velen por la protección de los datos en cualquier momento, tomando en consideración el conjunto de las situaciones sobrevenidas que puedan afectar al tratamiento de estos datos (e.g. fallo de seguridad, gestión de las solicitudes de rectificación o de acceso, cambio de prestador de servicios, entre otros).

Organizar los procesos conlleva:

- Tomar en consideración la protección de los datos personales desde el diseño;
- Sensibilizar y organizar al personal;
- Tratar las reclamaciones y las peticiones de los interesados en relación con el tratamiento de sus datos personales;
- Establecer un procedimiento para la correcta atención a las brechas de seguridad que deberán comunicarse a la Autoridad de control competente en un plazo máximo de 72 horas y, en determinadas ocasiones, incluso a los afectados.

FASE 6.- ADAPTAR LA DOCUMENTACIÓN EXISTENTE

a) Forma de recabar el consentimiento en cada uno de los tratamientos:

Las empresas deben revisar aquellos consentimientos obtenidos con anterioridad y verificar si cumplen con las nuevas exigencias del RGPD. En particular, sólo estarán legitimados aquellos prestados a través de una declaración o clara acción afirmativa. Por el contrario, el consentimiento no será considerado válido y la empresa deberá optar por:

- Abstenerse de tratar dichos datos y proceder a suprimirlos, o
- Recabar nuevamente el consentimiento de los afectados mediante procedimientos conformes con el RGPD.

Serán válidos y podrán seguir siendo utilizados los consentimientos que fueron prestados por el interesado a través de una manifestación de voluntad libre, específica, informada e inequívoca por medio de una declaración o clara acción afirmativa.

No serán válidos y deberán ser recabados de nuevo los consentimientos que fueron recabados mediante el silencio o la inacción del interesado.

b) Revisar las cláusulas informativas y establecer medidas complementarias de información:

Se incrementan los requisitos en cuanto al deber de informar a las personas interesadas añadiendo disposiciones adicionales. En este sentido, los clausulados deberán contener además los siguientes aspectos:

- Los datos de contacto del Delegado de Protección de Datos, cuando fuera necesario;
- La base jurídica o legitimación del tratamiento;
- El plazo y criterios de conservación de la información;

- Previsión de transferencias internacionales;
- Derecho a presentar una reclamación ante las Autoridades de Control;
- Posibilidad de ejercitar los derechos de los interesados (acceso, rectificación, supresión, limitación del tratamiento, portabilidad de los datos, oposición, a no ser objeto de decisiones individuales automatizadas), y;
- Existencia de decisiones automatizadas o elaboración de perfiles.

Los procedimientos, modelos o formularios existentes en la empresa y diseñados de conformidad con la LOPD, deberán ser revisados y adaptados antes de que el RGPD resulte de plena aplicación.

c) Contratos entre Responsables y Encargados del Tratamiento:

La organización deberá revisar los contratos de encargo del tratamiento mediante los cuales terceros ajenos a la empresa tengan acceso a datos personales de la empresa, modificando algunas cláusulas según el siguiente detalle:

- Medidas de seguridad: realizar un previo análisis de riesgos y determinar las medidas de seguridad a aplicar en función del tratamiento.
- Derechos de los interesados: se han incrementado respecto a los tradicionales derechos ARCO.
- Notificación de violaciones de seguridad: prever un procedimiento para la notificación de las violaciones de seguridad.

FASE 7.- DOCUMENTAR EL CUMPLIMIENTO

Para acreditar el cumplimiento del RGPD, la organización debe disponer de la documentación necesaria. Las acciones y los documentos elaborados en cada uno de los pasos deben ser revisados y actualizados regularmente para asegurar el cumplimiento de la normativa de protección de datos.

En este sentido, la empresa debe constituir un expediente documental, físico o electrónico, que le permita demostrar que los tratamientos de datos personales que efectúa se realizan cumpliendo con la normativa y se aplican las medidas técnicas y organizativas correspondientes.

El expediente deberá contener al menos los siguientes elementos:

La documentación sobre los tratamientos de datos personales llevados a cabo:

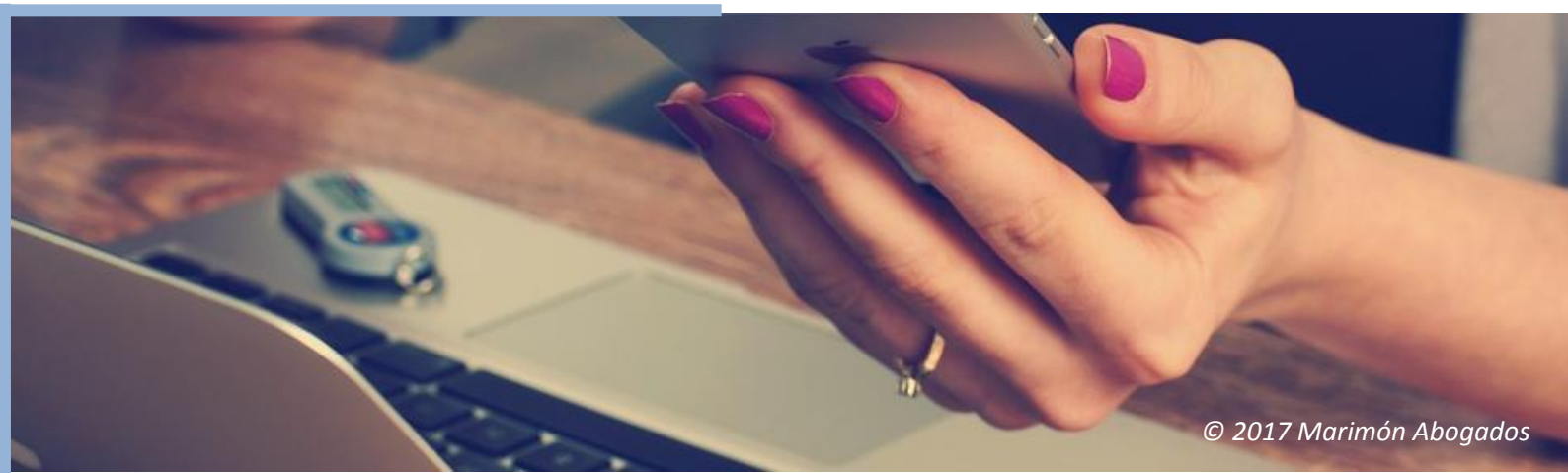
- El registro de actividad del tratamiento;
- Las evaluaciones de impacto sobre la protección de los datos;
- La documentación necesaria que habilite las transferencias internacionales de datos.

La información de las personas:

- Los documentos de información al interesado;
- Los modelos donde se recabe el consentimiento de los interesados;
- Los procedimientos implementados para el ejercicio de los derechos de las personas.

Los distintos contratos y acuerdos:

- Los contratos con los encargados del tratamiento;
- Los procedimientos internos en caso de violaciones de seguridad;
- Las pruebas de que los interesados prestaron previamente su consentimiento al tratamiento de sus datos personales.



LUIS MARIMÓN

lmarimon@marimon-abogados.com

Socio en Marimón Abogados. Forma parte del departamento de Derecho mercantil y es responsable del área de IT/IP.

EDUARD BLASI

blasi@marimon-abogados.com

Abogado Sénior en Marimón Abogados. Miembro del departamento especializado en IT/IP y experto en protección de datos.

Barcelona
Paseo de Gracia, 118
08008 Barcelona.
Tel.:+34 93 415 75 75
Fax:+34 93 415 83 11

Madrid
Paseo de Recoletos, 16
28001 Madrid.
Tel.: +34 91 310 04 56
Fax: +34 91 702 36 36

Sevilla
Balbino Marrón, 3
Planta 5ª-17 (Edificio Viapol)
41018 Sevilla.
Tel.: +34 954 657 896