C/M/S/
Law.Tax

Reglamento General de Protección de Datos: dos años de *accountability*

CMS España

25 de mayo de 2020

Reglamento General de Protección de Datos: dos años de *accountability*

Javier Torre de Silva, José Luis Piñar y Miguel Recio

El 25 de mayo de 2020 se cumplen dos años de la aplicación efectiva del Reglamento General de Protección de Datos (RGPD), que supuso pasar de un modelo basado en la comprobación del cumplimiento a otro centrado en la responsabilidad proactiva (*accountability*).

La Comisión Europea tendrá que emitir un informe sobre la evaluación y revisión del RGPD. Tras el primer informe, en 2020, se emitirá uno cada cuatro años.

Nuestros expertos han elaborado esta guía práctica en la que ofrecen algunas recomendaciones para asegurar y mejorar de manera continua el cumplimiento de la normativa sobre protección de datos. Además, se incluye acceso a algunos recursos digitales sobre el RGPD elaborados por CMS.

Índice

1. ¿Qué ha significado la aplicación efectiva del RGPD?

El 25 de mayo de 2018, fecha de aplicación efectiva del RGPD, implicó un punto de inflexión para quienes tratan datos personales, ya sean responsables o encargado del tratamiento, tanto del sector privado como público. Esta evolución se concreta en haber pasado pasar del control del cumplimiento (*compliance checklist*) a la **previa evaluación o valoración de los riesgos a los que pueda dar lugar el tratamiento de los datos personales (*risk based approach*)** para, a partir de los mismos, determinar qué **medidas técnicas y organizativas** (conocidas también como TOMs, por ser las siglas en inglés de *technical and organisational measures*).

Conocer los tratamientos de datos personales que se llevan a cabo en la organización y los riesgos derivados de estos tratamientos es esencial para poder adoptar una política o programa de protección de datos que, basado, en procedimientos o protocolos y controles efectivos, permitan garantizar el derecho fundamental a la protección de datos.

Tanto la política de protección de datos, cuando sea posible, como los procedimientos y controles efectivos deberán servir para demostrar el cumplimiento con la normativa sobre protección de datos a partir de la **responsabilidad proactiva** (*accountability*).

El RGPD ha introducido también **nuevas obligaciones y oportunidades** para las organizaciones que tratan datos personales. Desde la evaluación de impacto relativa al a protección de datos (EIPD) como "*un proceso concebido para describir el tratamiento, evaluar su necesidad y proporcionalidad y ayudar a gestionar los riesgos para los derechos y libertades de las personas físicas derivados del tratamiento de datos personales evaluándolos y determinando las medidas para abordarlos*" (Grupo de Trabajo del artículo 29, WP 248 rev.01); la figura del **delegado de protección de datos** en el caso de España y de otros Estados miembros; la desaparición de notificaciones de ficheros a las autoridades de protección de datos, si bien es necesario llevar un registro interno de tratamientos de datos personales o la obligación de notificar brechas de seguridad que afecten a los datos personales.

Nos encontramos, por tanto, en una fase en la que las organizaciones que tratan datos personales deberían contar ya con un **nivel de madurez en materia de protección de datos** que les permita, entre otras cuestiones, poder obtener certificaciones aprobadas y poder demostrar que han adoptado las medidas técnicas y organizativas adecuadas en atención al riesgo existente.

2. Algunas cifras destacables en materia de protección de datos

Las cifras pueden ayudar a dimensionar el significado y alcance de algunas cuestiones en materia de protección de datos.

En España una fuente relevante es la Memoria anual de la Agencia Española de Protección de Datos (AEPD), siendo la última la correspondiente al año 2019 (publicada en mayo de 2020). A la vista de esta Memoria, cabe destacar el hecho de que durante 2019 la AEPD recibió 11.590 reclamaciones en materia de protección de datos, siendo las más frecuentes las relativas a servicios de Internet, videovigilancia, inclusión indebida en ficheros de morosidad y reclamación de deudas; el traslado de reclamaciones a los responsables del tratamiento para que las atendiese aumentó un 147%, pasando de 2.300 a 5.691 y los procedimientos transfronterizos aumentaron un 33%.

Durante el año 2019 las resoluciones sancionadoras fueron 338. También durante el año pasado se impusieron 112 multas por un importe total de 6,2 millones de euros.

A finales de 2019 se habían notificado a la AEPD 50.326 delegados de protección de datos, de los que 44.069 se habían nombrado en el sector privado y 6.257 en el sector público.

Y si se presta atención, en particular, a las cifras mensuales publicadas por la AEPD (disponible aquí), durante el mes de abril de 2020 se notificaron 99 brechas de seguridad de los datos personales, lo que supone un aumento con respecto al mes previo, pero casi la mitad que en febrero de 2020. Por tipo de notificación, se dividieron en inicial (38) adicional (14) y completa (47) y, por sectores, 91 fueron del sector privado y 8 del sector público.

3. ¿En qué hemos avanzado y qué está todavía pendiente?

Tras dos años de aplicación efectiva del RGPD, y de prácticamente más de año y medio de la entrada en vigor de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPGDD), cabría considerar que es un buen momento para llevar a cabo una auditoría bienal del nivel de cumplimiento para asegurarse que las medidas técnicas y organizativas son efectivas; identificar si hay algún incumplimiento (*gap*), que requiera medidas de remediación, e identificar también oportunidades de mejora.

Se trata de tener un programa de cumplimiento o política de protección de datos, que deberá responder en todos los casos a la realidad de la organización, es decir, a su actividad diaria y a los tratamientos que lleve a cabo, con la finalidad de poder seguir una estrategia que optimice el nivel de cumplimiento y evite o minimice riesgos derivados del tratamiento de los datos personales, al mismo tiempo que debe estar alineada con la ciberseguridad.

A partir de lo anterior, una política de protección de datos, que debe haber sido adoptada por el máximo nivel de la organización y contar con su apoyo efectivo y constante, deberá servir para cumplir y demostrar el cumplimiento en todo momento. Los procedimientos y controles, actuales o futuros, están destinados a que la organización cuente con un gobierno y gestión adecuados de la protección de datos personales y que estén alineados con otras áreas o dimensiones, tales como el uso de las Tecnologías de la Información y las Comunicaciones (TIC) o la ciberseguridad.

Además, la protección de datos personales, como derecho fundamental, está interrelacionada también con la protección de los consumidores y la competencia, de manera que dependiendo de cuál sea la realidad de la organización tendrá que haber adoptado, o en su caso adoptar, medidas técnicas y organizativas. Y, en este sentido, en lugar de limitarse a cumplimentar una lista de cumplimiento o *checklist*, se trata de prestar a qué se ha hecho, cómo se ha hecho y qué queda por hacer, siendo así proactivamente responsable.

4. Doce medidas para cumplir y demostrar el cumplimiento que requieren de mejora continua

Cumplir, en este caso con la normativa sobre protección de datos, no se limita a una acción puntual, sino que requiere de una atención diaria.

Si consideramos que el 25 de mayo de 2018 era la fecha en la comenzaba la aplicación efectiva del RGPD, porque nunca se trató de una fecha límite (*deadline*) ni de entrega o finalización del proyecto de adecuación o implantación del RGPD; resulta necesario mantener y, si fuera necesario, ir actualizando las medidas técnicas y organizativas adoptadas. Claros ejemplos de que la fecha indicada era en la que comenzaba todo son el hecho de que todavía pueda revisarse si hay contratos con encargados del tratamiento que tienen que adecuarse al RGPD y a la LOPDGDD, que haya sido necesario identificar cuáles es la base de legitimación para el tratamiento de datos de salud relativos al COVID-19, que haya sido necesario adoptar medidas para cumplir con la normativa sobre protección de datos en

el control de registro horario o que se ha revisado cualquier cambio en el riesgo que implica el tratamiento de datos personales.

Incluso cuando se trate de medidas que ya se habían adoptado antes del 25 de mayo de 2018, todas las medidas técnicas y organizativas requieren de mejora continua, lo cual está estrechamente vinculado a la responsabilidad proactiva, con independencia de que una lista de cumplimiento o *checklist* pudiera servir como instrumento para no olvidar ninguna, más que para darlas por cumplidas.

En este sentido, se incluyen a continuación algunas recomendaciones o recordatorios, que podrían tenerse en cuenta antes de afrontar la auditoría bienal a la que hemos referencia anteriormente, y que podría ser considerada como una buena práctica para demostrar que se es responsable de manera proactiva.

1. Política de protección de datos y responsabilidad proactiva

El RGPD es la primera norma europea en materia de protección de datos en al que se incluye una referencia expresa y específica a políticas internas que, además, en el caso de las normas corporativas vinculantes se convierten en un elemento esencial para la aprobación de aquéllas por la autoridad competente de protección de datos.

La política de protección de datos, cuando sea posible su adopción, es un instrumento relevante para demostrar las medidas adoptadas para cumplir y poder demostrar el cumplimiento (*accountability*), siempre que sean medidas basadas en controles adecuados y efectivos. Esta política, que tiene que ser adoptada por dirección o el más alto nivel de la organización, no puede limitarse a una declaración de intenciones, sino que soporta todo el programa de cumplimiento en materia de protección de datos.

Algunas recomendaciones relevantes en relación con la política de protección de datos son:

— Adecuación a los tratamientos que se llevan a cabo en la organización, de manera que tenga en cuenta los procedimientos o procesos implementados, así como los controles adoptados.

— Revisión periódica de la política atendiendo a novedades legislativas, regulatorias y/o jurisprudencias, así como a directrices, orientaciones o sanciones de la autoridad de protección de datos.

— Difusión entre quienes tratan datos personales para el desarrollo de sus funciones y tareas en la organización. Y, al mismo tiempo, prueba de que se ha dado a conocer a quienes tratan datos personales.

— Formación y concienciación sobre la necesidad de que todo tratamiento de datos personales cumpla con esta política.

— Exigencia a los encargados del tratamiento de un nivel de protección de datos que no sea inferior al previsto en la política de protección de datos para poder cumplir y demostrar cumplimiento con la normativa y regulación aplicables.

2. Información al interesado: políticas de protección de datos y *cookies*

Aunque la información al interesado era una obligación, y un derecho del interesado, antes del RGPD, es necesario que las cláusulas y políticas de protección de datos (utilizadas para informar sobre el tratamiento de los datos personales), cumplan con los requisitos de los artículos 13 (datos personales obtenidos del interesado) y 14 del RGPD (datos personales no obtenidos del interesado).

En el caso de Internet, la AEPD ha prestado especial atención a la denominada como política de protección de datos o política de privacidad, que no debe confundirse con el documento interno indicado en el apartado previo, dando lugar a la publicación de su Informe sobre políticas de privacidad en Internet, adaptación al RGPD (Septiembre 2018).

Al respecto, son recomendaciones relevantes:

— Considerar la posibilidad de información por capas o información básica y restante información.

— Asegurarse de que cualquier cambio en el tratamiento o nuevo tratamiento de datos personales se incluyan en la cláusula informativa y/o política de protección de datos o privacidad.

— Revisar periódicamente que todas las cláusulas informativas incluidas en formularios, cupones, contratos, correo electrónico o proporcionada por teléfono y/o política de protección de datos o privacidad publicada en la web de la organización está actualizada y cumple con los requisitos necesarios.

— Revisar que los carteles informativos sobre el uso de videocámaras u otros dispositivos similares (GPS, *drones*, etc.) cumplen con los requisitos necesarios.

— Facilitar la información sobre el tratamiento de los datos personales cuando se ejerza el derecho de acceso.

Sin perjuicio de lo anterior, el uso de *cookies* quedará también sujeto al RGPD y a la LOPDGDD cuando dé lugar a un tratamiento de datos personales. Al respecto, la AEPD publicó una versión actualizada de su Guía sobre el uso de las *cookies* (disponible aquí), con la colaboración de varias asociaciones del sector de la publicidad, en la que explican, entre otras cuestiones, los diferentes tipos de *cookies* y cómo cumplir con las obligaciones en materia de transparencia y obtención del consentimiento, cuando este último sea necesario.

Además, la guía incluye las responsabilidades de las diferentes partes que intervienen en el uso de *cookies* y también un anexo con el esquema de los principales actores que pueden intervenir en la compra digital de publicidad programática.

3. Bases de legitimación del tratamiento

Para ser lícito, todo tratamiento de datos personales requiere de una base de legitimación del tratamiento. Si no existe una base de legitimación del tratamiento, este sería ilícito. El RGPD establece un listado de posibles bases de legitimación, siendo el responsable del tratamiento quien tiene que identificar la que corresponda, salvo que estuviera ya determinada, por ejemplo, en una ley que prevea que los datos serán necesarios para cumplir con un contrato en el que el interesado sea parte, cumplir con una obligación legal o el ejercicio de poderes públicos conferidos al responsable del tratamiento.

Si los datos que se tratan son alguna de las categorías especiales de datos previstos en el RGPD y que son los relativos a salud, opiniones políticas o afiliación sindical, hay que tener en cuenta que su tratamiento está prohibido salvo que, además de tener una base de legitimación, concurra alguna de las circunstancias previstas en el artículo 9.2 del RGPD.

En relación con las bases de legitimación del tratamiento, sería conveniente considerar:

— La forma y gestión del consentimiento. El consentimiento tendrá que ser expreso y, en algunos casos tales como el relativo a las categorías especiales de datos, explícito. Además, el responsable del tratamiento tiene que poder demostrar que obtuvo el consentimiento necesario cuando este sea la base de legitimación.

— Si el tratamiento se basa en el interés legítimo, es necesario realizar la ponderación entre los intereses del responsable del tratamiento y los intereses y derechos fundamentales de del interesado, informar al interesado de cuál es el interés legítimo y de la ponderación hecha, así como documentar dicha ponderación.

— Revisar que las bases de legitimación estén incluidas para cada finalidad en la cláusula informativa y/o en la política de protección de datos o privacidad.

— En el caso del inventario a publicar por las Administraciones Públicas y otros responsables o encargados del tratamiento indicados en el artículo 77.1 de la LOPDGDD, revisar que las bases de legitimación han sido incluidas y que están actualizadas.

— Si se tratan datos de menores de catorce años, considerar las cuestiones específicas que se plantean en cada caso, en particular cuando el tratamiento se basa en el consentimiento o en el interés legítimo.

4. Una lista ampliada de derechos de los interesados

Con finalidad de que la persona física tenga un mayor control sobre sus datos personales, el RGPD introdujo nuevos derechos, tales como los de portabilidad, derecho al olvido y limitación del tratamiento, además de actualizar otros. El ejercicio de los derechos implica que el responsable del tratamiento tenga que adoptar medidas para **gestionar las solicitudes de ejercicio de derechos sobre protección de datos** en tiempo y forma.

La falta de atención o gestión inadecuada de las solicitudes de ejercicio de derechos podría dar lugar a que el interesado solicite la tutela de la autoridad de protección de datos competente. Por ejemplo, una respuesta dada después del plazo de un mes desde haber recibido la solicitud correspondiente, y cuando no se hubiera informado de la necesidad de una prórroga debido a la complejidad y número de solicitudes, supondría un incumplimiento de la normativa sobre protección de datos. Además, dado que la lista de derechos se amplió, el responsable del tratamiento tendría que haber considerado estos nuevos derechos.

Las recomendaciones relevantes para el responsable del tratamiento en materia de derechos de los interesados y gestión de las solicitudes que reciba son:

— Revisar que las cláusulas informativas y/o políticas de protección de datos o privacidad han sido actualizadas para incluir todos los derechos, incluido el relativo a la presentación de una reclamación ante la autoridad de protección de datos (indicando cuál es) si se considera que el tratamiento de los datos infringe la normativa aplicable.

— Haber actualizado el procedimiento o protocolo que se utilice para gestionar (recibir, analizar y dar respuesta) a las solicitudes de ejercicio de derechos, incluido el uso que se haga de la tecnología (por ejemplo, un formulario web, posibilidad de que el usuario pueda ejercer sus derechos a través del acceso a su cuenta, etc.).

— Tener en cuenta los límites al ejercicio de derechos, tales como que no afecten a terceras personas, y cómo actuar en caso de solicitudes manifiestamente excesivas o infundadas.

— Considerar que la gestión de solicitudes de ejercicio de derechos es un tratamiento más que tiene que cumplir con los requisitos aplicables en materia de protección de datos.

— Asegurarse de tener firmado un contrato u otro acto jurídico con el encargado del tratamiento si se ha encomendado a alguien externo o a otra empresa del grupo la gestión de las solicitudes de ejercicio de derechos.

5. Plazos de conservación y bloqueo de los datos personales

Uno de los principios de licitud del tratamiento de los datos personales es el relativo a la limitación del plazo de conservación durante el tiempo que sea necesario para cumplir con la finalidad o finalidades del tratamiento. El responsable del tratamiento tiene que identificar el plazo correspondiente, informando al interesado de dicho plazo o de los criterios utilizados para determinarlo.

La LOPDGDD incluye una previsión adicional, que es la relativa al bloqueo de los datos. Esta obligación consiste en que adoptar medidas técnicas y organizativas que impidan el tratamiento de los datos personales, excepto para ponerlas a disposición de las autoridades competentes, en particular las de protección de datos, durante el plazo de prescripción de las posibles responsabilidades derivadas del tratamiento de los datos.

En particular el responsable del tratamiento debería considerar los siguientes aspectos:

— Revisar que ha identificado todos los plazos o criterios para determinar los plazos de conservación de los datos personales y considerar los medios utilizados para el tratamiento de los datos (bases de datos, correo electrónico, etc.).

— Si se ha adoptado un procedimiento de conservación de datos personales, comprobar que esté actualizado.

— Cuando se vayan a rectificar o suprimir datos personales, cumplir con la obligación de bloqueo adoptando las medidas técnicas y organizativas necesarias de manera que los datos personales únicamente queden a disposición de las autoridades competentes.

— Comprobar que todas las cláusulas informativas y/o políticas de protección de datos o privacidad a través de las que se informe a los interesados sobre el tratamiento de los datos personales incluyen el correspondiente plazo o criterios para determinar el plazo de conservación de los datos personales.

— Como parte del procedimiento de supresión, borrado o anonimización de los datos personales, es necesario adoptar medidas adecuadas, tales como el borrado seguro o técnicas de anonimización robustas.

6. Revisión de contratos con encargados del tratamiento

En muchos casos, antes de la aplicación efectiva del RGPD ya se habían firmado contratos u otros actos jurídicos con encargados del tratamiento que tienen acceso a datos personales para prestar algún servicio al responsable del tratamiento.

Al respecto, la LOPDGDD prevé que en el caso de contratos con encargados del tratamiento suscritos antes del 25 de mayo de 2018 con fecha (a) señalada en los mismos, mantengan su vigencia hasta entonces, momento en el que deberán adecuarse al RGPD y a la LOPDGDD y (b) indefinida, se adecúen al RGPD y a la LOPDGDD antes del 25 de mayo de 2022. No obstante, durante estos plazos cualquiera de las partes podrá exigir a la otra la adecuación del contrato al RGPD ya la LOPDGDD.

Con carácter general, por lo que se refiere a los contratos con encargados del tratamiento, sería recomendable:

— Revisar que todo tratamiento de datos personales en el que intervenga un encargado del tratamiento tiene el correspondiente contrato u otro acto jurídico que cumpla con los requisitos del RGPD y de la LOPDGDD.

— Considerar las fechas indicadas en la LODPGDD para revisar los contratos con encargados del tratamiento que se hubieran firmado antes del 25 de mayo de 2018.

— Asegurarse de que solo se recurre a encargados del tratamiento que ofrecer garantías suficientes para que el responsable del tratamiento cumpla y pueda demostrar el cumplimiento de la normativa aplicable sobre protección de datos.

— Si no se utiliza un modelo o estándar que se proporcione a los encargados del tratamiento para su firma, haber establecido y mantener un procedimiento de revisión de los contratos facilitados por los encargados para asegurarse de que incluyen todos los requisitos necesarios.

— En el registro de actividades del tratamiento, vincular el tratamiento de los datos personales con el correspondiente contrato de encargado del tratamiento.

7. Más opciones para las transferencias internacionales de datos

Ya sea porque la empresa tiene su matriz o subsidiarias en otros países alrededor del mundo, porque se utilizan servicios digitales para el tratamiento de datos personales, tales como la nube, o porque es necesario en el ámbito de las Administraciones Públicas, las transferencias internacionales de datos han aumentado exponencialmente durante los últimos años.

Debiendo tener en cuenta que la Directiva 95/46/CE es previa a la expansión de Internet y la oferta de muchos servicios digitales que han surgido en los últimos años, el RGPD introduce nuevas opciones para las transferencias internacionales de datos, tales como los códigos de conducta y certificaciones aprobadas. También aclara cuáles son los supuestos que requieren o no de autorización previa de la autoridad de protección de datos competente.

Las principales recomendaciones sobre las transferencias internacionales de datos tras dos años de aplicación efectiva del RGPD son:

— Valorar las diferentes opciones (cláusulas contractuales tipo, BCrs, etc.) previstas en el RGPD si se van a realizar transferencias internacionales de datos.

— Si se hubieran firmado para realizar transferencias a la matriz o subsidiarias en otros países, revisar los contratos o acuerdos intragrupo para verificar que incluyen los requisitos del RGPD.

— Si la organización tuviera la necesidad de realizar transferencias incluso a países sin nivel adecuado, considerar la posibilidad de obtener la aprobación de las normas corporativas vinculantes (*Binding Corporate Rules*, BCRs).

— Si se transfieren datos personales de personas trabajadoras a un tercer país sin nivel adecuado, revisar cuál es la base de legitimación del tratamiento y las garantías adecuadas para llevar a cabo dicha transferencia internacional.

— Revisar que tanto la cláusula informativa como el registro de actividades del tratamiento incluyen, específicamente, la información necesaria sobre las garantías en las que se basa la transferencia internacional de datos.

8. Análisis del riesgo

Como consecuencia de la evolución hacia la responsabilidad proactiva, el RGPD se ha basado en la aproximación basada en el riesgo, lo que da lugar a que quienes tratan datos personales identifiquen y evalúen el riesgo que implique el tratamiento de los datos personales para adoptar e implementar medidas técnicas y organizativas adecuadas.

Se trata de una acción que no es puntual, sino que requiere considerar cualquier cambio en el riesgo derivado, por ejemplo, de cambios en la finalidad del tratamiento, amenazas para la seguridad de los datos personales o cambios normativos o regulatorios. Esto implica que quienes tratan datos personales, como responsable o encargado del tratamiento, tengan que revisar el riesgo cuando sea necesario, de manera proactiva.

En relación con esta obligación, algunas recomendaciones relevantes son:

— Comprobar que todo tratamiento de datos personales ha sido objeto de análisis de riesgos para determinar las medidas técnicas y organizativas, incluidas las de seguridad, aplicables.

— Prestar atención a cualquier cambio o nuevo riesgo en relación con el tratamiento de datos personales. Debe considerarse también que el riesgo es constante y cambiante.

— Calcular el riesgo inherente y residual que exista en todo tratamiento de datos personales.

— Evaluar qué medidas técnicas y organizativas desde la perspectiva del riesgo legal y técnico.

— Documentar y guardar un registro del análisis de riesgos llevado a cabo.

9. Evaluación de impacto relativa a la protección de datos

Aunque es una obligación introducida por el RGPD, cuando el tratamiento de datos personales implique un alto riesgo para la persona física, no es algo nuevo ya que se encontraba en la Directiva 95/46/CE. A diferencia del análisis de riesgos, que se centra en la determinación de las medidas técnicas y organizativas por la organización que trata datos personales, la evaluación de impacto relativa a la protección de datos (EIPD) presta especial atención al impacto que tiene el tratamiento de los datos personales para los derechos y libertades fundamentales de la persona física.

Sobre si hay que hacer o no una EIPD, además de las directrices publicadas por el Comité Europeo de Protección de Datos, cabe señalar que la Agencia Española de Protección de Datos publicó una Guía práctica para las evaluaciones de impacto relativas a la protección de datos (disponible aquí) y dos listados. El primer listado incluye el listado de tipos de tratamientos de datos que requieren una EIPD (disponible aquí) y el segundo es un listado orientativo de tratamientos que no quieren de una EIPD (disponible aquí). Además, la AEPD publicó un modelo de informe de informe de EIPD tanto para el sector público (disponible aquí) como para el sector privado (disponible aquí).

Las recomendaciones relevantes cuando sea necesario hacer una EIPD son:

— Elegir o adoptar una metodología adecuada, que responda a la realidad de la organización, para el desarrollo de la EIPD, pudiendo desarrollarse una metodología propia.

— Contar con el asesoramiento del DPD, debiendo tener en cuenta que quien tiene que realizar la EIPD es el responsable del tratamiento.

— Asegurarse de que en los contratos con los encargados del tratamiento se han incluido previsiones específicas para obtener la información que pudiera ser necesaria sobre el tratamiento de los datos personales por este para realizar la EIPD.

— Considerar la posibilidad de compartir información, por ejemplo a través de un informe de EIPD, sin que esto afecte a información protegida por secretos empresariales o comerciales, derechos de autor, etc., o revele vulnerabilidades.

— Documentar toda EIPD realizada o que se realice, de manera que se pueda demostrar su realización, con lo que esto supone para la responsabilidad proactiva.

10. Designación del DPD y notificación a la autoridad de protección de datos

Aunque la figura del DPD contaba ya con un amplio recorrido en otros Estados miembros de la Unión Europea, tales como Alemania o Francia, se convirtió en una novedad en nuestro país. Tanto si su designación es obligatoria como voluntaria, el DPD desempeña funciones y tareas clave por lo que se refiere a supervisar el cumplimiento de la organización en materia de protección de datos.

Por lo que se refiere a esta figura que ha cumplido también dos años en España como consecuencia de la aplicación efectiva del RGPD, es recomendable:

— Asegurar que el DPD participa en todas las reuniones u otras acciones en las que se traten cuestiones relativas a protección de datos personales.

— Que se haya designado por escrito del DPD, en la que se incluyan, entre otros aspectos, sus funciones, tareas y datos de contacto, así como la comunicación a toda la organización.

— Cuando sea necesario, que se ha evaluado cualquier posible conflicto de interés y, en todo caso, mantener la independencia del DPD, tanto funcional como orgánica.

— Proporcionar al DPD el apoyo necesario para que pueda realizar sus funciones de manera independiente.

— Comprobar que se ha procedido a comunicar la designación o cualquier cambio en la designación del DPD a la autoridad de protección de datos que sea competente.

11. Comunicación de brechas de seguridad de los datos personales

Una brecha de seguridad, según las definiciones dadas en el RGPD, es "*toda violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos*".

La obligación de notificar a la autoridad de protección de datos competente las brechas o violaciones de seguridad que afecten a los datos personales, cuando impliquen un riesgo para los derechos y libertades fundamentales de los interesados, así como de comunicarla a los afectos cuando implique un alto riesgo, es una de las nuevas obligaciones para muchos responsables del tratamiento.

El tiempo que ha transcurrido desde la aplicación efectiva del RGPD sirve para hacer algunas recomendaciones relevantes en la materia:

— Designar a una persona o equipo de personas de contacto tanto ante la autoridad de protección de datos como de los afectados.

— Comprobar que en los contratos con encargados del tratamiento de han incluido obligaciones específicas al respecto de manera que el responsable pueda cumplir con sus correspondientes obligaciones.

— Considerar la guía publicada por la Agencia Española de Protección de Datos, el procedimiento electrónico existente, así como los formularios electrónicos para la notificación de brechas de seguridad de las autoridades autonómicas, según la que sea competente en cada caso.

— Revisar que el procedimiento interno establecido en caso de que ocurra una brecha de seguridad sea efectivo.

— Mantener un registro interno de brechas de seguridad de los datos personales que sirva para cumplir también con la obligación de documentarlas.

12. Actualización del registro de actividades del tratamiento y publicación por Administraciones Públicas

El registro de actividades del tratamiento, en los casos previstos en el RGPD para responsables y encargados del tratamiento, fue una de las nuevas obligaciones introducidas en 2018. Este registro es también una herramienta que permite tanto a la organización como al DPD, si hubiera sido designado de manera obligatoria o voluntaria, a poder tener identificados todos los tratamientos de datos personales que se llevan a cabo en la organización.

Elaborar el registro de actividades del tratamiento es el primer paso ya que es necesario mantenerlo actualizado a lo largo del tiempo. Este registro de actividades del tratamiento deberá estar por escrito, inclusive por medios electrónicos.

Algunas recomendaciones relevantes sobre el registro de actividades del tratamiento son:

— Asegurarse de que el registro de actividades del tratamiento contiene toda la información exigible y está actualizado.

— Establecer un procedimiento para la revisión y actualización periódica del registro de actividades del tratamiento.

— Tener un procedimiento o protocolo para comunicar internamente cambios en el registro de actividades del tratamiento como consecuencia de nuevos tratamientos de datos personales, cambios en los encargados del tratamiento, etc.

— Tener el registro de actividades en el idioma de la autoridad de protección de datos que pueda solicitarlo.

— En el caso de responsables y encargados del tratamiento a los que se refiere el artículo 77.1 de la LOPDGDD (Administraciones Públicas y otros órganos constitucionales, grupos parlamentarios, etc.), comprobar que los inventarios de datos publicados están debidamente actualizados para incluir toda la información de los tratamientos que se lleven a cabo.

5. Tres acciones relevantes en materia de protección de datos

Después de dos años de responsabilidad proactiva toda organización que trate datos personales debería tener ya un programa o política interna de protección de datos que le permita cumplir y demostrar el cumplimiento en materia de protección de datos.

A partir de los tratamientos de datos personales que llevan a cabo, la identificación del riesgo derivado de estos tratamientos y de las medidas técnicas y organizativas aplicables, se trata de que la organización sea proactiva y no reactiva o limitarse a la comprobación del cumplimiento.

En cualquier caso, las tres acciones principales a tener en cuenta por quienes tratan datos personales ya sean responsables, corresponsables o encargados del tratamiento, son:

→ **Supervisar de manera constante que las medidas técnicas y organizativas son adecuadas en atención al riesgo y que el programa de protección de datos está alineado con los tratamientos que se llevan a cabo en la organización.**

→ **Apoyar al DPD en el desempeño de sus funciones y considerar la conveniencia de designarlo de manera voluntaria.**

→ **Formar y concienciar en materia de protección de datos y seguridad de los datos personales a quienes los traten para el desarrollo de sus funciones.**

6. Directrices del Comité Europeo de Protección de Datos

El Comité Europeo de Protección de Datos (CEPD), creado por el RGPD y al que se incorporó el Grupo de Trabajo del artículo 29, adoptó como propias alguna de las directrices emitidas por este último y ha seguido publicando otras directrices y dictámenes con interpretaciones sobre algunas cuestiones tales como el consentimiento, la evaluación de impacto relativa a la protección de datos, la transparencia, las brechas de seguridad de los datos personales, la autoridad líder, etc.

Además de las directrices y dictámenes, el CEPD publica otros documentos relevantes, tales como decisiones vinculantes, cartas enviadas a otras autoridades, directrices sobre la Directiva (UE) 2016/680 sobre protección de datos personales en el ámbito policial y judicial en materia penal, los códigos de conducta y certificaciones aprobadas o las normas corporativas vinculantes.

Las directrices del CEPD sobre el RGPD pueden consultarse aquí.

7. Guías de la Agencia Española de Protección de Datos

Durante los dos últimos años, e incluso unos meses antes de la fecha de aplicación efectiva del RGPD, la Agencia Española de Protección de Datos (AEPD) ha publicado, y continúa haciéndolo, diversas guías, así como infografías y herramientas, dirigidas a los responsables y encargados del tratamiento.

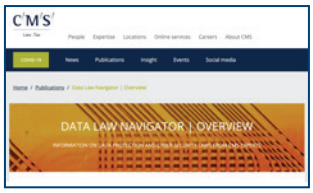
Desde herramientas como Facilita RGPD y el canal INFORMA_RGPD, dirigido a PYMEs, hasta orientaciones a las Administraciones Públicas (disponibles aquí) y a empresas en general (disponibles aquí). De esta manera la AEPD ofrece guías, recomendaciones, infografías y otros contenidos que debe conocer quien trata datos personales.

A la AEPD se suman también las autoridades autonómicas de protección de datos (Andalucía, Cataluña y País Vasco), que en su respectivo ámbito territorial son competentes en el caso del sector público autonómico y local.

8. Algunos recursos relevantes sobre protección de datos y ciberseguridad de CMS

1. *CMS Data Law Navigator*

El *CMS Data Law Navigator* proporciona una visión general sobre las legislaciones en materia de protección de datos y ciberseguridad en más de treinta países alrededor del mundo, entre los que se encuentra España. Es una herramienta fundamental para poder entender el marco normativo y regulatorio en materia de protección de datos y ciberseguridad.



Se trata de un recurso de información que se actualiza periódicamente y al que se puede acceder aquí.

2. *GDPR Enforcement Tracker*

CMS ofrece también la herramienta *GDPR Enforcement Tracker*.

Es un sitio web (disponible aquí) que ofrece una lista de las resoluciones sancionadoras más relevantes publicadas por las autoridades de protección de datos en los Estados miembros desde el 25 de mayo de 2018.

La herramienta ofrece la posibilidad de buscar resoluciones por varios campos (país, autoridad de protección de datos, tipo de infracción), además de poder realizar búsquedas en general. Y también es posible obtener algunas estadísticas como, por ejemplo, número acumulado de multas impuestas y suma de las sanciones.

3. Guías y otras publicaciones sobre protección de datos

Desde el departamento de TMC de CMS Albiñana & Suárez de Lezo publicamos constantemente guías, artículos de fondo y posts sobre cuestiones de actualidad y relevantes en materia de protección de datos personales.

Algunas de estas guías son la de protección de datos y teletrabajo (disponible aquí), la de obligaciones y cuestiones a tener en cuenta sobre protección de datos y ciberseguridad cuando se desarrollan apps (disponible aquí) o la de la incidencia del COVID-19 en la protección de datos de carácter personal (disponible aquí).

Entre los artículos de fondo cabe destacar el relativo a la celebración de reuniones *online* por órganos de gobierno y administración de personas jurídicas y protección de datos de carácter personal (disponible aquí).

Además, habitualmente publicamos posts jurídicos en los que abordamos cuestiones de interés en materia de protección de datos y ciberseguridad, tales como si un contrato electrónico entre el responsable y el encargado del tratamiento para cumplir con el requisito de un contrato por escrito; la nueva Guía de la AEPD en materia de *cookies* y tecnologías similares o sobre el derecho al olvido. Y también apariciones en los medios de comunicación para opinar o informar sobre cuestiones de máxima actualidad.

Para más información, puede contactar con el equipo de TMC de CMS Albiñana & Suárez de Lezo:

Javier Torre de Silva
Socio | TMC / Protección de Datos

T +34 91 451 93 21
E javier.torredesilva@cms-asl.com

José Luis Piñar
***Of Counsel* | TMC / Protección de Datos**

T +34 91 451 40 53
E joseluis.pinar@cms-asl.com

Miguel Recio
Asociado | TMC / Protección de Datos

T +34 91 452 01 90
E miguel.recio@cms-asl.com

La presente publicación no constituye asesoramiento jurídico de sus autores.

cms-asl@cms-asl.com | **cms.law**