GlobalSTD CERTIFICATION

EL RGPD – UE – 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO, DE 26.04.2016, EN ESPAÑA.
MEDIDAS DE RESPONSABILIDAD PROACTIVA

En este artículo se presenta en alto nivel el Reglamento General de Protección de Datos en España (RGPD, o GDPR, por sus siglas en inglés, General Data Protection Regulation).

A continuación se citan dos elementos de carácter general que constituyen la mayor innovación del RGPD para las organizaciones, proyectándose sobre todas las obligaciones de las mismas: el principio de responsabilidad proactiva y el enfoque al riesgo para los derechos y libertades de las personas cuyos datos son tratados.

EL RGPD EN ESPAÑA

En España y, en general, en la Unión Europea (UE), el Reglamento General de Protección de Datos (RGPD) entró en vigor en mayo de 2016; siendo aplicable desde el 25 de mayo de 2018.

El gobierno español presentó ante el Congreso de Diputados el proyecto en noviembre de 2017, manifestando una tramitación parlamentaria más demorada de lo deseado, sin contar a estas alturas con una ley de adaptación al nuevo marco jurídico europeo; para el 25 de mayo de 2018 solo Alemania, Austria y Reino Unido tenían aprobadas sus respectivas leyes.

Algunas cuestiones necesitaban ser reguladas para hacer efectiva la protección de datos y, en particular, la actividad de supervisión y control (como venía manifestando la Agencia Española de Protección de Datos), que con su Directora Mar España al frente, está llevando a cabo una labor ímproba y ejemplar para facilitar al máximo el tránsito al nuevo modelo de privacidad que el reglamento trae consigo, basado en la responsabilidad proactiva y el enfoque al riesgo de quienes manejan datos personales.

Para agilizar la situación y mientras no se apruebe la nueva Ley Orgánica, el Gobierno ha aprobado el Real Decreto Ley 5/2018, publicado en el BOE del 30 de julio de 2018. La norma no regula el contenido esencial del derecho a la protección de datos porque no puede hacerlo, pero sí regula cuestiones relevantes como la inspección en materia de protección de datos, el régimen sancionador y los procedimientos en caso de una posible vulneración de la normativa sobre protección de datos. Además atribuye a la Agencia Española de Protección de Datos la representación ante el Comité Europeo de Protección de Datos, regulando la publicación de las resoluciones de la Agencia y el régimen transitorio, tanto de procedimientos como de la adecuación de contratos de encargo del tratamiento.

El cambio que el Reglamento trae consigo en el ámbito de procedimientos y sanciones es capital, los primeros pueden internacionalizarse en el ámbito de la Unión Europea (procedimientos transfronterizos) y las segundas se incrementan notablemente (hasta 20 millones de euros), por lo que era imprescindible regular la actividad investigadora, la tramitación de procedimientos de reclamación, la prescripción de infracciones y sanciones, la colaboración con las autoridades de protección de datos del resto de los países de la Unión Europea y la determinación del alcance territorial (nacional o europeo) de los procedimientos. En resumen, el Real Decreto Ley 5/2018 es esencial para la plena aplicabilidad del nuevo marco europeo de protección de datos, ahora sólo falta que la nueva ley sea aprobada cuanto antes.

En esta regulación el legislador decidió utilizar la figura del Reglamento, dada la dispar transposición por parte de cada Estado Miembro a la Directiva 95/46 (en España supuso el desarrollo de la Ley 15/99 el 13 de diciembre, de protección de datos de carácter personal y el RD 1720/2007 el 21 de diciembre), disparidad que generaba inseguridad jurídica, además de la percepción generalizada de la existencia de riesgos en la protección de las personas físicas, especialmente en lo relacionado al tráfico de datos de carácter personal a través de Internet. Así fue como se apostó por una regulación que pudiera ser directamente aplicable a todos los Estados Miembros, dejando así un escaso margen a la regulación a nivel nacional.

El RGPD es pues una norma directamente aplicable a todos los Estados Miembros, con la misma categorización que las leyes emanadas de los parlamentos nacionales, no requiriendo de normas internas de transposición, ni de normas de desarrollo o aplicación (en la mayoría de los casos), surtiendo efecto pleno sin necesidad de que se dicten normas nacionales. Cabe señalar que un reglamento europeo relega la aplicación de cualquier norma nacional que contraponga lo dispuesto en él.

Por ello, los responsables deben asumir que la norma de referencia es el RGPD y no las normas nacionales, como venía sucediendo hasta ahora con la Directiva 95/46. No obstante, la futura ley que sustituirá a la actual Ley Orgánica de Protección de Datos en España, LOPD, Ley 15/99, del 13 de diciembre, sí podrá incluir algunas precisiones o desarrollos en materias que permite el RGPD; mismo que señala expresamente qué determinados puntos sean decididos de forma definitiva por los Estados Miembros, siendo la razón de que tenga que existir también una nueva ley nacional de protección de datos en cada uno de los Estados Miembros. **Lo que aplica es el RGPD y, completando el esquema, la ley nacional.*

El RGPD contiene obligaciones que deben ser analizadas y aplicadas por cada organización, tomando en cuenta sus propias circunstancias. Estas obligaciones se cumplirán, porque el respeto de un derecho fundamental como la protección de datos personales es un valor en sí mismo, además de evitar sanciones económicas o bien porque el daño reputacional de no hacerlo es inasumible. En este sentido, dos elementos de carácter general constituyen la mayor innovación del RGPD para los responsables y se proyectan sobre todas las obligaciones de las organizaciones: el principio de responsabilidad proactiva y el enfoque de riesgo para los derechos y libertades de las personas cuyos datos son tratados.

|Principio de la responsabilidad proactiva

El RGPD describe este principio como la necesidad de que el responsable del tratamiento aplique medidas técnicas y organizativas apropiadas, con el fin de garantizar y poder demostrar que el tratamiento es conforme al RGPD.

En términos prácticos, este principio requiere que las organizaciones analicen qué datos tratan, con qué finalidades lo hacen y qué tipo de operaciones de tratamiento llevan a cabo (Registro de Actividades de Tratamiento, RAT). A partir de este conocimiento, deben describir la forma en que aplicarán las medidas que el RGPD prevé, asegurándose de que son las adecuadas para cumplir con el mismo y que pueden demostrarlo ante los interesados y las autoridades de supervisión.

En síntesis, este principio exige una actitud consciente, diligente y proactiva por parte de las organizaciones frente a todos los tratamientos de datos personales que lleven a cabo (Registro de Actividades de Tratamiento, RAT).

|Enfoque de riesgo para los derechos y libertades de las personas

El RGPD señala que las medidas dirigidas para garantizar su cumplimiento deben tener en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento, así como el riesgo para los derechos y libertades de las personas. De acuerdo con este enfoque, algunas de las medidas que el RGPD establece se aplicarán sólo cuando exista un alto riesgo para los derechos y libertades, mientras que otras deberán modularse en función del nivel y tipo de riesgo que los tratamientos presenten.

Por lo tanto, la aplicación de las medidas previstas por el RGPD debe adaptarse a las características de las organizaciones. Lo que puede ser adecuado para una organización que maneja datos de millones de interesados en tratamientos complejos que involucran información personal sensible o volúmenes importantes de datos sobre cada afectado.
**No es necesario para una pequeña empresa que lleva a cabo un volumen limitado de tratamientos de datos no sensibles.*

CUMPLIR CON EL RGPD
DELEGADO DE PROTECCIÓN DE DATOS

Cumplir con el Reglamento General de Protección de Datos de la Unión Europea no es sencillo y conlleva costes. En algunos casos implica la obligación de designar a un Delegado de Protección de Datos (DPD o DPO, por sus siglas en inglés: Data Protection Officer).

El DPD es un profesional que cuenta con la experiencia y formación que exige el Esquema de Certificación de la Agencia Española de Protección de Datos (AEPD), cuya función consiste en coordinar y controlar el cumplimiento del RGPD en las organizaciones.

En relación a las **medidas de responsabilidad activa** que permitirían asegurar razonablemente el cumplimiento de los principios, garantías y derechos establecidos en el reglamento, el propio RGPD establece que los responsables, y en ocasiones los encargados, deben aplicar para garantizar que los tratamientos que realizan son conformes con el reglamento y están en condiciones para demostrarlo.

|Análisis de riesgo

El RGPD condiciona la adopción de medidas de responsabilidad activa ante los riesgos que los tratamientos puedan presentar para los derechos y libertades de los interesados.

Se maneja el riesgo de dos maneras:

- En algunos casos, determina las medidas que deberán aplicarse solo cuando el tratamiento suponga un alto riesgo para los derechos y libertades *(como evaluaciones de impacto sobre la protección de datos).*

- En otros casos, las medidas deberán modularse en función del nivel y tipo de riesgo que conlleve el tratamiento *(como con las medidas de protección de datos desde el diseño o con las medidas de seguridad).*

Todos los responsables deberán realizar una valoración de riesgo sobre los tratamientos que realizan, a fin de establecer las medidas que deben aplicarse y cómo deben hacerlo.

El tipo de análisis variará en función de:

- Los tipos de tratamiento.
- La naturaleza de los datos.
- El número de interesados afectados.
- La cantidad y variedad de tratamientos que una misma organización lleve a cabo.

En las grandes organizaciones, como regla general, el análisis deberá realizarse mediante alguna de las metodologías de análisis de riesgo existentes. Por ejemplo, aplicar un MAGERIT a un análisis organizacional que enfoque el análisis de riesgos en lugar de los procesos sobre las amenazas derivadas de los datos de carácter personal que intervienen en las actividades, afecta a cada uno de los procesos en términos de confidencialidad, integridad, disponibilidad, cumplimiento legal, entre otros.

En organizaciones de menor tamaño y con tratamientos de poca complejidad, el análisis será el resultado de una reflexión mínimamente documentada sobre las implicaciones de los tratamientos en los derechos y libertades de los interesados; la reflexión deberá dar respuesta a cuestiones como las que se exponen en el listado siguiente. **A mayor número de respuestas afirmativas, mayor será el riesgo que podría derivarse del tratamiento. Si la respuesta a estas preguntas y otras del mismo tipo fuera negativa, es razonable concluir que la organización no realiza tratamientos que generen un elevado nivel de riesgo y que, por tanto, no debe poner en marcha las medidas previstas para esos casos.*

- ¿Se tratan datos sensibles?
- ¿Se incluyen datos de una gran cantidad de personas?
- ¿El tratamiento incluye la elaboración de perfiles?
- ¿Se cruzan los datos obtenidos de los interesados con otros disponibles en otras fuentes?
- ¿Se pretende utilizar los datos obtenidos para una finalidad ajena a la principal?
- ¿Se están tratando grandes cantidades de datos que incluyan técnicas de análisis masivo tipo big data?
- ¿Se utilizan tecnologías especialmente invasivas para la privacidad, como las relativas a geolocalización, videovigilancia a gran escala o aplicaciones del Internet de las Cosas?

|Registro de actividades de tratamiento | RAT

Los responsables y encargados deberán mantener un registro de las operaciones de tratamiento en el que se contenga la información que establece el RGPD, como:

- Nombre y datos de contacto del responsable y delegado de protección de datos (si existiese).
- Finalidades del tratamiento.
- Descripción de categorías de los interesados y de los datos personales tratados.
- Cesiones.
- Transferencias internacionales de datos.

El Reglamento General de Protección de Datos exime a las pequeñas y medianas empresas (PYME) de la obligación de elaborar Registros de Actividades de Tratamiento de datos personales, salvo que el tratamiento que se realice por la PYME pueda entrañar un riesgo para los derechos y libertades de los interesados, no sea ocasional, o incluya categorías especiales de datos personales o análogas. En la práctica, esta redacción lleva a que muchas PYMES se planteen si están obligadas o no a mantener un RAT.

El Grupo de Trabajo del Artículo 29 **(GT29)** acaba de publicar su informe de posición en relación a la mencionada excepción (artículo 30.5 RGPD). Dicho informe GT29 interpreta el RGPD en el sentido de confirmar la obligación de elaborar un RAT para pymes que se encuentren en alguna de las tres circunstancias que desactivan la excepción. Si bien, aclara que este RAT solo deberá referirse a las actividades de tratamiento afectadas por la casuística mencionada. Es decir, introduce como novedad la desagregación del RAT, pudiendo ser necesario realizarlo únicamente en determinadas actividades. Así, por ejemplo, una entidad que exclusivamente lleve a cabo el tratamiento de datos personales derivados de la gestión de nóminas, solo deberá contar con un RAT que comprenda el tratamiento referido a dicho proceso, puesto que ese tratamiento es, por definición, recurrente y, en consecuencia, habitual o no ocasional.

El RAT es el elemento esencial para una gestión estructurada de la información, tanto a nivel interno como de cara a los eventuales requerimientos de la autoridad de control. Además, resulta una herramienta muy útil para que las entidades adquieran una **visión integral de las actividades de tratamiento** que llevan a cabo para que esta nueva perspectiva redunde en una mayor congruencia de la **estrategia de privacidad corporativa.**

En líneas generales, el artículo 30 del RGPD establece un contenido mínimo para los RAT tanto de responsables como de encargados del tratamiento. Por ahora, ni el Proyecto de la nueva LOPD ni la Agencia Española de Protección de Datos han planteado una propuesta de estructura para el RAT, lo cual ha creado incertidumbre en las entidades, especialmente en aquellas Pymes que se puedan encontrar en una zona gris sobre si pueden acogerse o no a la excepción prevista en el artículo 30.5 del RGPD.

La **Autoridad Bávara** de Protección de datos publicó en marzo de este año una guía para la elaboración del RAT. Esta guía es la única existente sobre el RAT hasta la fecha.

Sobre el RAT, la guía bávara apunta una serie de cuestiones menores en apariencia pero de gran relevancia práctica, como la obligación de conservar un historial de modificaciones del RAT por un periodo, en virtud del principio de responsabilidad proactiva establecido en el artículo 5.2 del RGPD. Este historial resulta necesario de cara a establecer una trazabilidad en las modificaciones realizadas en el RAT a lo largo del periodo.

En relación al artículo 30.5, la Autoridad Bávara indica que se trata de una excepción de aplicación limitada, siendo habitual que una PYME concurra en la casuística que impide activar la excepción, sobre todo porque, bien trata datos personales de manera recurrente o bien trata datos sensibles.

|Protección de datos desde el diseño y por defecto

Estas medidas se incluyen en las que debe aplicar el responsable con anterioridad al inicio del tratamiento y también cuando se esté desarrollando. Este tipo de medidas reflejan muy directamente el enf que de responsabilidad proactiva. Se trata de pensar en términos de protección de datos desde el mismo momento en que se diseña un tratamiento, un producto o servicio que implica el tratamiento de datos personales. Desde el inicio, los responsables deben tomar medidas organizativas y técnicas para integrar en los tratamientos garantías que permitan aplicar de forma efectiva los principios del RGPD.

Los responsables deben adoptar medidas que garanticen que solo se traten los datos necesarios en lo relativo a la cantidad de datos tratados, la extensión del tratamiento, periodos de conservación y accesibilidad a datos.

|Medidas de seguridad

El Reglamento de Desarrollo de la Ley 15/99 del 13 de diciembre, de protección de datos de carácter personal, RD 1720/2007, de 21 de diciembre, determinaba con detalle y de forma exhaustiva las medidas de seguridad que debían aplicarse según el tipo de datos objeto de tratamiento. En el RGPD, los responsables y encargados establecerán las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado en función s los riesgos detectados en el análisis previo.

Las medidas del Reglamento de la Ley 15/99 del 13 de diciembre, de protección de datos de carácter personal estaban basadas casi exclusivamente en el tipo de datos que se trataban, con alguna matización relativa al contexto en que se llevaban a cabo los tratamientos. El RGPD pide que se tomen en consideración más variables.

Las medidas técnicas y organizativas deberán establecerse tomando en cuenta:

- Costo de la técnica.
- Costos de aplicación.
- Naturaleza, alcance, contexto y fines del tratamiento
- Riesgos para los derechos y libertades.

El esquema de medidas de seguridad previsto en el Reglamento de Desarrollo de la Ley 15/99 del 13 de diciembre, de protección de datos de carácter personal, RD 1720/2007, del 21 de diciembre, dejó de tener validez de forma automática el 25 de mayo de 2018.

En algunos casos los responsables podrán seguir aplicando las mismas medidas que establece el RD 1720/2007, si los resultados del análisis de riesgos previo concluyen que las medidas son realmente las más adecuadas para ofrecer un nivel de seguridad adecuado. En ocasiones será necesario completarlas con medidas adicionales o prescindir de alguna de las medidas.

Pongamos un ejemplo:
En referencia a las novedades introducidas por el Reglamento en materia laboral, debemos mencionar que se mantiene la regla general según la que el tratamiento de datos será lícito y no requerirá del consentimiento expreso del empleado si es necesario para la ejecución de su contrato laboral, manteniendo en todo caso el deber de informar al trabajador sobre el tratamiento de sus datos. No obstante, la nueva norma amplía los extremos sobre los que habrá que facilitar la información al trabajador, exigiendo que la información se proporcione de una forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo.

Refiriéndonos más concretamente al control de acceso o de presencia basado en el uso de datos biométricos del empleado (esto son aquellos que permitan o confirmen la identificación única de su titular, como el reconocimiento de imágenes faciales o del iris, e incluso de voz, datos dactiloscópicos, entre otros) cada vez más habituales en las empresas, dada la seguridad que ofrecen al empresario y la comodidad que supone para el empleado, que no debe depender de tarjetas de acceso u otros instrumentos fácilmente extraviables (herramientas técnicas que se están imponiendo como sistemas asimilables a una firma electrónica, especialmente en dispositivos móviles). A diferencia del régimen aplicable en la Ley 15/99, el Reglamento categoriza los datos biométricos como especialmente protegidos, exigiendo para su tratamiento un mayor nivel de diligencia y mayores obligaciones de seguridad que en la vigente ley de protección de datos.

La base jurídica para el tratamiento de tales datos, por el momento deberá ser el consentimiento prestado por el empleado, por lo que en los casos en que no otorgue ese consentimiento, se deberán utilizar mecanismos alternativos para identificar sus accesos a las instalaciones de la empresa. No obstante, el Reglamento prevé que tales datos puedan tratarse en el marco del cumplimiento de obligaciones y en el ejercicio de derechos específicos del responsable del tratamiento o del trabajador en el ámbito del derecho laboral y de seguridad social, en medida que lo autorice el Derecho de la Unión de los Estados Miembros o un convenio colectivo, con arreglo al Derecho de los Estados Miembros, que establezca garantías adecuadas para los derechos fundamentales e intereses del involucrado.

Pensando en Facebook y basándonos en esta argumentación, estaría incumpliendo la norma al tener activa, por defecto, la captación y tratamiento de datos biométricos. Lo adecuado es que la red social deshabilite este sistema y permita su activación en caso que el usuario europeo desee otorgar este consentimiento.

Los datos biométricos han sido elevados a una categoría especial, poniéndolos al mismo nivel de protección que los de carácter sanitario. Además, para poder realizar cualquier tipo de tratamiento, se deberá pedir un consentimiento explícito e individual. El artículo 9.1 del RGPD explica que queda prohibido el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, convicciones religiosas y los datos genéticos y biométricos, dirigidos para identificar de manera unívoca a una persona física (siendo ésta la gran novedad) o datos relativos a la salud.

Todas las entidades o redes sociales que quieran hacerse con los datos biométricos de los usuarios y tratarlos deberán solicitar un consentimiento individual para poder hacerlo, por lo que ya no valdrá aceptar los términos y condiciones genéricos El que pretenda hacer un tratamiento de estos datos especialmente protegidos deberá explicar claramente lo que va a hacer con ellos y conseguir un permiso claro y manifiesto del usuario.

Pero, ¿qué medidas deben implementar las empresas y a quién afectará la nueva normativa de protección de datos de la UE? La respuesta no es del todo clara, el Reglamento no plantea unas órdenes específicas pero explica que se deberán aplicar los mismos niveles de protección que los que se implementan para los datos sanitarios, como el cifrado de la información o imponer medidas de seguridad técnicas que impidan el acceso a terceros. Sea como sea, lo que sí que es evidente es que lo apuntado en el RGPD es de aplicación a las compañías de la Unión Europea y a todas las empresas extranjeras que tengan algún tipo de negocio en la UE.

Existe muy poca información con respecto a los datos biométricos y son pocos los que entienden la importancia de los mismos, puesto que son asimilables a una firma electrónica que podría dar, virtualmente, acceso a cualquier información, ya sea personal o bancaria. Por esa razón, los expertos creen que las instituciones europeas de protección de datos deben realizar un mayor esfuerzo de divulgación sobre los peligros del mal uso de los datos biométricos, debiéndose imponer a todos los niveles la privacidad desde el diseño, como solicita el RGPD.

Por ello, habrá que estar atento a las novedades legislativas que puedan darse en la materia para determinar cuál será la base jurídica que legitimará dicho tratamiento por parte de las empresas.

| Notificación de "violaciones a la seguridad de datos"

El RGPD define las violaciones de seguridad de datos (comúnmente conocidas como "quiebras de seguridad") de una forma muy amplia, que incluye todo incidente que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, además de la comunicación o acceso no autorizado a dichos datos. Sucesos como la pérdida de un ordenador portátil, el acceso no autorizado a las bases de datos de una organización (incluso por su propio personal) o el borrado accidental de algunos registros constituyen violaciones de seguridad del RGPD y deben ser tratadas como el Reglamento establece.

Cuando se produzca una violación a la seguridad de datos, el responsable debe notificarla a la autoridad de protección de datos competente, a menos que sea improbable que la violación suponga un riesgo para los derechos y libertades de los afectados.

La notificación de la quiebra a las autoridades debe producirse sin dilación indebida y, a ser posible, dentro de las 72 horas siguientes en las que el responsable tenga constancia de ella.

La notificación ha de incluir en su contenido mínimo:

- Naturaleza de la violación.
- Categorías de datos y de los interesados afectados.
- Medidas adoptadas por el responsable para solventar la quiebra.
- Si procede, las medidas aplicadas para paliar los posibles efectos negativos sobre los interesados.

Los responsables deben documentar todas las violaciones de seguridad; en los casos que sea probable que la violación entrañe un alto riesgo para los derechos o libertades de los interesados, la notificación a la autoridad de supervisión deberá complementarse con un aviso dirigido a estos últimos.

El objetivo de la notificación a los afectados es permitir que puedan tomar medidas para protegerse de sus consecuencias. Por ello, el RGPD requiere que se realice sin dilación indebida, sin hacer referencia ni al momento en que se tenga constancia de ella ni tampoco a la posibilidad de efectuar la notificación dentro de un plazo de 72 horas. El propósito es siempre que el interesado afectado pueda reaccionar tan pronto como sea posible.

El RGPD añade a los contenidos de la notificación las recomendaciones sobre las medidas que pueden tomar los interesados para hacer frente a las consecuencias de la quiebra.

La valoración del riesgo de la quiebra es distinta al análisis de riesgos previo a todo tratamiento. Se trata de establecer hasta qué punto el incidente (por sus características), el tipo de datos a los que se refiere o el tipo de consecuencias que puede tener para los afectados, puede causar un daño en sus derechos o libertades.

Los daños pueden ser materiales o inmateriales, e ir desde la posible discriminación de los afectados como consecuencia de su uso por quien ha accedido a ellos de forma no autorizada hasta la usurpación de identidad, pasando por perjuicios económicos o la exposición pública de datos confidenciales.

Se considera que se tiene constancia de una violación de seguridad cuando hay certeza de que se ha producido y se tiene un conocimiento suficiente de su naturaleza y alcance.

La mera sospecha de que ha existido una quiebra o la constatación de que ha sucedido algún tipo de incidente sin que se conozcan mínimamente sus circunstancias no deberían dar lugar todavía a la notificación, dado que en esas condiciones no sería posible, en la mayoría de los casos, determinar hasta qué punto puede existir un riesgo para los derechos y libertades de los interesados.

En casos de quiebras que por sus características pudieran tener gran impacto, sí podría ser recomendable contactar con la autoridad de supervisión tan pronto como existan evidencias de que se ha producido alguna situación irregular en la seguridad de los datos, sin perjuicio de que esos primeros contactos puedan completarse con una notificación formal más completa dentro del plazo legalmente previsto.

Puede haber casos en que la notificación no pueda realizarse dentro de esas 72 horas, por ejemplo, por la complejidad en determinar completamente su alcance. En esos casos, es posible hacer la notificación con posterioridad, acompañándola de una explicación de los motivos que han ocasionado el retraso. **La información puede proporcionarse de forma escalonada cuando no sea posible hacerlo en el mismo momento de la notificación.*

El criterio de alto riesgo debe entenderse en el sentido de que sea probable que la violación de seguridad ocasione daños de entidad a los interesados. Por ejemplo, en los casos que se desvele información confidencial, como contraseñas o participación en determinadas actividades, se difundan de forma masiva datos sensibles o se puedan producir perjuicios económicos para los afectados.

La notificación a los interesados no será necesaria cuando:

- El responsable haya tomado medidas técnicas u organizativas apropiadas con anterioridad a la violación de seguridad, en particular las que hagan ininteligibles los datos para terceros, como el cifrado.
- El responsable haya tomado con posterioridad a la quiebra medidas técnicas que garanticen que ya no hay posibilidad de que el alto riesgo se materialice.
- Cuando la notificación suponga un esfuerzo desproporcionado, teniendo que ser sustituida por medidas alternativas, como una comunicación pública.

Notificación de quiebras de seguridad a la AEPD: *https://sedeagpd.gob.es/sede-electronica-web/vistas/formBrechaSeguridad/procedimientoBrechaSeguridad.jsf*

|Evaluación de Impacto sobre la Protección de Datos

Los responsables del tratamiento deberán realizar una Evaluación de Impacto sobre la Protección de Datos (EIPD) previamente a la puesta en marcha de aquellos tratamientos que tengan la posibilidad de conllevar un alto riesgo para los derechos y libertades de los interesados.

El RGPD establece un contenido mínimo de las Evaluaciones de Impacto sobre la Protección de Datos, aunque no contempla ninguna metodología específica para su realización. Cuando el análisis de riesgos de las organizaciones sobre los tratamientos indique que presentan un alto riesgo para los derechos o libertades de los interesados, los responsables deberán realizar una EIPD sobre esos tratamientos, a fin de estar en condiciones de adoptar las medidas adecuadas para incorporar esos tratamientos a las exigencias del RGPD.

En los casos que las EIPD hayan identificado un alto riesgo que, a juicio del responsable de tratamiento no pueda mitigarse por medios razonables en términos de tecnología disponible y costes de aplicación, el responsable deberá consultar a la autoridad de protección de datos competente. La consulta debe ir acompañada de la documentación que prevé el RGPD, incluyendo la propia Evaluación de Impacto, y la autoridad de supervisión puede emitir recomendaciones o ejercer cualquier otro de los poderes que el RGPD le confiere, entre ellos el de prohibir la operación de tratamiento.

Una lista indicativa de supuestos en la que se considera que los tratamientos conllevan un alto riesgo podría tener:

- Elaboración de perfiles sobre los que se toman decisiones que produzcan efectos jurídicos en los interesados o les afecten significativamente de modo similar.
- Tratamientos a gran escala de datos sensibles.
- Observación sistemática a gran escala de una zona de acceso público.

Según el Grupo del Artículo 29, en su designación de Delegados de Protección de Datos, para valorar si un tratamiento se realiza a gran escala debe tomar en cuenta:

- El número de interesados afectados, tanto en términos absolutos como en proporción de una determinada población.
- El volumen de datos y la variedad de datos tratados.
- La duración o permanencia de la actividad de tratamiento.
- La extensión geográfica de la actividad de tratamiento.

Las autoridades de protección de datos están obligadas a confeccionar listas adicionales de tratamientos que requerirán una EIPD.

La existencia de estos listados no excluye que los responsables deban realizar el análisis de riesgos correspondiente y, en caso de que concluyan que existe un alto riesgo para los derechos y libertades de los interesados, se desarrolle una EIPD, aún cuando el tratamiento en cuestión no esté incluido en la lista mencionada. Como se ha dicho, el RGPD se basa en un principio de responsabilidad activa y es siempre en último extremo el responsable el que debe decidir qué medidas aplicar y cómo hacerlo. La intervención de las autoridades de supervisión o las previsiones del propio RGPD aclaran sus disposiciones o las especifican, pero no sustituyen la responsabilidad de quienes tratan los datos.

Es posible realizar una única EIPD para varios tratamientos similares que entrañen altos riesgos también similares, puede ser necesario llevar a cabo una nueva evaluación cuando cambien las condiciones del tratamiento o cuando varíen los riesgos asociados al mismo.

|Delegado de Protección de Datos

El RGPD establece la figura del Delegado de Protección de Datos (DPD), que será obligatorio en:

- Autoridades y organismos públicos.
- Responsables o encargados que tengan entre sus actividades principales las operaciones de tratamiento que requieran una observación habitual y sistemática de interesados a gran escala.
- Responsables o encargados que tengan entre sus actividades principales el tratamiento a gran escala de datos sensibles.

El DPD se nombrará atendiendo a sus competencias profesionales y, en particular, a su conocimiento de legislación y práctica de la protección de datos.

Aunque no debe tener una titulación específica, en la medida que entre las funciones del DPD se incluya el asesoramiento al responsable o encargado en todo lo relativo a la normativa sobre protección de datos, los conocimientos jurídicos en la materia son sin duda necesarios, pero también es necesario contar con conocimientos ajenos a lo estrictamente jurídico, como en materia de tecnología aplicada al tratamiento de datos o en relación al ámbito de actividad de la organización en la que el DPD desempeña su tarea.

La designación del DPD y sus datos de contacto deben hacerse públicos por los responsables y encargados, y deberán ser comunicados a las autoridades de supervisión competentes.

La posición del DPD en las organizaciones tiene que cumplir con los requisitos establecidos, entre los que se encuentran:

- Total autonomía en el ejercicio de sus funciones.
- Necesidad de relacionarse con el nivel superior de la dirección.
- Obligación de que el responsable o el encargado faciliten al DPD todos los recursos necesarios para desarrollar su actividad.

Se permite nombrar un solo DPD para un grupo empresarial siempre que sea accesible desde cada establecimiento del grupo. La accesibilidad debe entenderse en un sentido amplio; incluye la accesibilidad física para el propio personal del grupo y también la posibilidad de que los interesados contacten al DPD en su lengua, aun cuando esté adscrito a un establecimiento en otro Estado Miembro.

La AEPD ha optado por promover un sistema de certificación de profesionales de protección de datos como una herramienta útil a la hora de evaluar que los candidatos para el puesto de DPD tengan las cualificaciones profesionales y conocimientos requeridos.

Las certificaciones serán otorgadas por las entidades certificadoras debidamente acreditadas por la Entidad Nacional de Acreditación (ENAC), siguiendo criterios de acreditación y certificación elaborados por la AEPD en colaboración con los sectores afectados.

La certificación no será un requisito indispensable para el acceso a la profesión, será sólo una opción a disposición de los responsables y encargados para facilitar su selección de profesionales llamados a ocupar el puesto de DPD. Asimismo, los responsables y encargados pueden tomar en consideración otras cuestiones u otros medios para demostrar la competencia de los DPD.

Se permite que el DPD mantenga una relación laboral o mediante un contrato de servicios con los responsables o encargados, también permite que pueda contratarse el servicio de DPD con personas físicas o jurídicas ajenas a la organización. También está permitido que el DPD desarrolle sus funciones a tiempo completo o parcial, en este último caso es preciso evitar que existan conflictos de intereses. Estos conflictos pueden surgir cuando el DPD, en su tarea de supervisión de las actividades de tratamiento de datos llevadas a cabo por la organización, debe valorar su propio trabajo dentro de ella, como sucede si se designa como DPD al responsable de tecnologías de la información (cuando se emplean para el tratamiento de datos) o al responsable de un área de negocio que decide sobre determinados tratamientos.

El RGPD prevé también el catálogo de funciones del DPD, entre las que se incluyen las relativas a actuar como punto de contacto para los interesados en todo lo que tenga relación con el tratamiento de sus datos personales.

|Transferencias Internacionales

El modelo de transferencias internacionales diseñado por el RGPD sigue los mismos criterios que el establecido por la Directiva 95/46 y por las legislaciones nacionales de trasposición.

Los datos solo podrán ser comunicados fuera del Espacio Económico Europeo:

- A países, territorios o sectores específicos (el RGPD incluye también organizaciones internacionales) sobre los que la Comisión haya adoptado una decisión, reconociendo que ofrecen un nivel de protección adecuado.
- Cuando se hayan ofrecido garantías adecuadas sobre la protección que los datos recibirán en su destino.
- Cuando se aplique alguna de las excepciones que permita transferir los datos sin garantías de protección adecuada por razones de necesidad, vinculadas al propio interés del titular de datos o a intereses generales.

Desde el punto de vista de los responsables y encargados que actualmente realizan transferencias internacionales o las efectúan en el marco del RGPD:

- Las decisiones de adecuación que la Comisión ha adoptado con anterioridad a la aplicación del RGPD seguirán siendo válidas, y por tanto, podrán seguir realizándose transferencias basadas en ellas, mientras que la Comisión no las sustituya o derogue.
- Las decisiones de la Comisión estableciendo cláusulas para los contratos en los que se establecen garantías para las transferencias internacionales seguirán siendo válidas hasta que las sustituya o derogue.
- Las autorizaciones de transferencias que las autoridades nacionales de protección de datos hayan otorgado sobre la base de garantías contractuales seguirán siendo válidas en tanto las autoridades no las revoquen.
- Las garantías sobre la protección que recibirán los datos en destino las debe ofrecer el exportador, que podrá ser tanto un responsable como un encargado de tratamiento.
- Se amplía la lista de posibles instrumentos para ofrecer garantías, incluyendo expresamente, entre otros, las Normas Corporativas Vinculantes para responsables y encargados, los códigos de conducta y esquemas de certificación, y las cláusulas contractuales que puedan aprobar las autoridades de protección de datos.

En los casos de las Normas Corporativas Vinculantes, cláusulas contractuales estándar, códigos de conducta y esquemas de certificación, la transferencia no requerirá la autorización de las autoridades de supervisión.

Se añade una excepción al listado que en su momento estableció la Directiva 95/46; se trata de la posibilidad de que el responsable pueda transferir datos a un país sin un nivel adecuado de protección cuando esa transferencia sea necesaria para satisfacer los intereses legítimos imperiosos del responsable, tomando en cuenta que la transferencia no sea repetitiva y que afecte solamente a un número limitado de interesados. En todo caso, la transferencia solo será posible si no prevalecen los derechos, libertades e intereses de los afectados, y deberá comunicarse a la autoridad de protección de datos.

El RGPD se refiere en varios lugares al tratamiento de los datos de **menores** (niños, en la terminología del RGPD); la mención más explícita está relacionada con la obtención del consentimiento en el ámbito de la oferta directa de servicios de la sociedad de la información. El RGPD prevé que en ese entorno, el consentimiento solo será válido a partir de los 16 años, debiendo contar con la autorización de los padres o tutores legales por debajo de esa edad. El RGPD permite a los estados miembros establecer una edad inferior, siempre que no sea menor a los 13 años.

Es de esperar que muchos estados miembros hagan uso de esta posibilidad y adopten regulaciones propias. En España, el Reglamento de Desarrollo de la Ley 15/99 define los 14 años con carácter general como la edad a partir de la que es válido el consentimiento de los menores. Por ello es razonable suponer que la norma que reemplace la Ley 15/99 contenga también una regulación específica en esta materia.

El Comité de Libertades Civiles del Parlamento Europeo ha formulado una propuesta de resolución para su aprobación en pleno, en la que pide a la Comisión Europea la suspensión del acuerdo Privacy Shield entre la Unión Europea y los Estados Unidos, el acuerdo entró en vigor desde julio de 2016 en virtud de facilitar la transferencia internacional de datos entre ambas zonas.

El Privacy Shield sustituyó al anterior acuerdo existente entre la Unión Europea y los Estados Unidos, denominado **Safe Harbor**, que fue anulado por sentencia del Tribunal de Justicia de la Unión Europea a raíz de una denuncia del ciudadano austriaco Maximillian Schrems ante la Agencia de Protección de Datos de Irlanda.

En el borrador de resolución del Comité de Libertades Civiles, el Parlamento Europeo da como plazo hasta

el 1 de septiembre de este año como recomendación para que se suspenda el *Privacy Shield* si no se acredita que los Estados Unidos cumplan plenamente con el Acuerdo Internacional, sugiriendo que se mantenga la suspensión en tanto no se acredite ese pleno cumplimiento.

De llevarse a cabo esta resolución, si se verifica la falta de adaptación de los Estados Unidos al *Privacy Shield*, el 1 de septiembre dejarían de ser válidas las transferencias de datos entre la Unión Europea y EE.UU basadas en el marco de ese Acuerdo, por lo que numerosas empresas tendrían que cesar en su actividad, si esta implicara la realización de tales transferencias. Es un escenario muy parecido al que se planteó hace poco más de dos años con la anulación del *Safe Harbor* por el Tribunal de Justicia de la Unión Europea (TJUE), lo que causó numerosos problemas en los negocios transcontinentales.

Esta recomendación, si bien es enormemente preocupante, no resulta sorprendente. La propia sentencia del TJUE sobre el *Safe Harbor* ya contenía una argumentación perfectamente aplicable a la situación actual. En esencia, el TJUE decía que si no existen garantías de que el país de destino en una transferencia internacional respeta los principios y derechos fundamentales de los europeos en materia de protección de datos, tales transferencias no se pueden realizar a ese país. En aquella ocasión se hacía referencia a los accesos generalizados a datos de europeos que realizaban las agencias de investigación americanas, que se habían puesto de manifiesto en los documentos que salieron a la luz a raíz de la **filtración de Snowden**, posibilitando injerencias por parte de las autoridades públicas estadounidenses en los derechos fundamentales de las personas. En el documento que ha salido ahora del Parlamento se hace referencia a casos recientes, como el de **Facebook** y **Cambridge Analytics**, señalando que ambas compañías están registradas en el marco del Privacy Shield y ello no ha evitado el mal uso de los datos, de lo que se deduce que ese marco no es suficientemente protector de los derechos de los interesados, porque no permite que las obligaciones de supervisión y control se estén ejercitando de forma adecuada.

Pero no hace falta acudir a casos tan mediáticos para ver que el Privacy Shield ya estaba afectado por serios problemas desde casi sus comienzos; podemos recordar que en enero de 2017, el recién nombrado presidente **Donald Trump**, en la primera Orden Ejecutiva que firmó tras su toma de posesión como primer mandatario de los EE.UU, bajo el título de "Aumento de la Seguridad Pública en el Interior de los EE.UU" ya decía que "Las agencias (*estatales*) deberán asegurar que sus políticas de privacidad excluyan de la protección de la Ley de Privacidad a personas que no sean ciudadanos de los EE.UU.…". Con esta declaración de intenciones resultaba patente que el contenido del *Privacy Shield* no casaba bien con tales principios.

El documento del Parlamento que ha salido a la luz cita también como un punto de preocupación la reciente aprobación en EE.UU de la ***"Clarifying Lawful Overseas Use of Data Act"***, conocida como la ***"CLOUD Act"***, que permite acceder a datos almacenados por empresas americanas en cualquiera que sea la ubicación de sus servidores, evitando así la necesidad de acudir a mecanismos de colaboración internacional a través de tratados de cooperación judicial.

Se divisa nuevamente un difícil horizonte para las transferencias internacionales entre Europa y EE.UU, es cierto que existen otros mecanismos para regular las transferencias internacionales en el recientemente aplicable Reglamento General de Protección de Datos de la Unión Europea (RGPD), pero el marco del *Privacy Shield* es muy cómodo porque evita tener que firmar documentos específicos para cada transacción que se produzca entre partes, facilita el cumplimiento de la obligación de informar y supone un marco estable de transferencias. Veremos si el Parlamento adopta la propuesta de resolución del Comité de Libertades, dado el escenario político existente no parece que podamos ser demasiado optimistas.

Estas medidas se completan con los derechos de los afectados con respecto al tratamiento de sus datos personales, la relación entre el responsable y el encargado de tratamiento, así como la legitimación para el tratamiento de datos personales.

GlobalSTD CERTIFICATION

CONTÁCTANOS

España

España y Portugal

C./ Serrano 209, 6ºD
28016 Madrid, España.

+00 34 91 188 01 02
+00 34 608 19 40 52