TEMA 7

RGPD

Reglamento General de Protección de Datos

MARIO ABAD, ALEJANDRO BAÑULS,
DANI MARTÍNEZ, PABLO MARTÍNEZ,
ÁNGEL PÉREZ

ÍNDICE

INTRODUCCIÓN

La Agencia Española de Protección de Datos (AEPD) fue creada en 1993. Es el organismo público que anteriormente velaba por el cumplimiento de la Ley Orgánica de Protección de Datos de Carácter Personal y su cumplimiento. El objetivo de esta ley es básicamente regular el tratamiento de datos y ficheros, de carácter personal. Hoy día, con la actualización de la ley a la RGPD, la AEPD sigue siendo la encargada de asegurar el cumplimiento de esta nueva ley.

El RGPD está basado en el principio de Accountability y marca unas pautas a seguir para conseguir una mayor seguridad, transparencia y consentimiento en la concesión y manejo de los datos personales. Toda aquella persona o empresa que maneje o almacene datos de carácter personal, por cuenta propia o de terceros, debe tomar ciertas medidas de seguridad para el tratamiento de estos, estos datos tienen distintos niveles de importancia, y en función de los datos que vayamos a manejar/almacenar se deben implementar las correspondientes medidas de seguridad para su protección.

El 25 de mayo de 2018 entró en vigor el 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 RGPD, que sustituyó la LOPD.

CONCEPTOS Y DEFINICIONES

DATOS PERSONALES

Como hemos mencionado anteriormente, dicho reglamento regula los datos de carácter general. Nos referimos a datos personales como cualquier información relativa a una persona física viva identificada o identificable, es decir, es cualquier información numérica, alfabética, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables, tanto la relativa a su identidad como la relativa a su existencia y ocupaciones.

En caso de que los datos personales hayan sido anonimizados, cifrados o presentados con un seudónimo, pero puedan seguir siendo utilizados para identificar a una persona, siguen siendo considerados datos personales y se recogen en el ámbito de aplicación del RGPD. En caso de que estos datos hayan sido anonimizados de forma que se pierda la capacidad identificar a la persona, dejan de considerarse como datos personales. Con el fin de que los datos se consideren verdaderamente anónimos, esta anonimización debe ser irreversible. El RGPD protege los datos personales independientemente de la tecnología

utilizada para su tratamiento, de forma que podemos decir que es “tecnológicamente neutro” y se aplica tanto en tratamiento automatizado como manual, siempre que los datos se organicen con arreglo a criterios predeterminados (como el orden alfabético).

Asimismo, no importa la forma en que se conservan los datos. Ya sea en un sistema informático, a través de videovigilancia o sobre papel, en todos estos casos, los datos personales están sujetos a los requisitos de protección establecidos en el RGPD.

Algunos ejemplos de datos personales:

- Nombre y apellidos
- Domicilio
- Dirección de correo electrónico, del tipo nombre.apellido@empresa.com
- Número de documento nacional de identidad
- Datos de localización (Por ejemplo, localización en un móvil)
- Dirección IP
- Identificador de una cookie
- Datos médicos

Algunos ejemplos de datos no considerados personales:

- Dirección de correo electrónico, del tipo info@empresa.com
- Datos anonimizados

Cabe mencionar que en algunos casos existe una legislación sectorial específica que regula, por ejemplo, el uso de los datos de localización o el uso de las cookies.

Dentro de los datos personales podemos encontrarnos determinados datos que por su relevancia e importancia para la privacidad deben ser tratados y almacenados con mayor cuidado. Nos referimos a ellos como datos sensibles.

Los datos que se consideran sensibles según el RGPD son los mismos que en la LOPD, añadiendo tres nuevos. Algunas de las categorías especiales son:

- Opiniones políticas
- Convicciones religiosas
- Origen racial
- Vida sexual
- Dato genético
- Dato biométrico
- Orientación sexual

En cuanto a los datos almacenados para nuestro proyecto de gestión de autónomos podemos proporcionar una serie de niveles de “seguridad”, aunque la GPDR dice que cada persona es responsable de cómo organizarlo, se aconseja seguir los niveles de la antigua LOPD.

- **Nivel alto:** Son ficheros o tratamientos de nivel alto, entre otros, los que se refieren a datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual. Una de las medidas de seguridad que se debe implantar en estos ficheros de nivel alto (si son automatizados) es, por ejemplo, la del registro de accesos, de manera que quede registrado el usuario que ha intentado acceder al fichero, la hora, el fichero, el tipo de acceso y si dicho acceso ha sido autorizado o denegado.

- **Nivel medio:** Son ficheros o tratamientos de nivel medio, entre otros, aquellos relativos a la prestación de servicios de solvencia patrimonial y créditos, aquellos de los que sean responsables entidades financieras para las finalidades relacionadas con la prestación de servicios financieros y aquellos que contengan un conjunto de datos que ofrezcan una definición de las características o de la personalidad y que permitan evaluar determinados aspectos de la personalidad o del comportamiento de las personas.

  Una de las medidas que se debe implantar para estos ficheros o tratamientos de datos de nivel medio es la realización de una auditoría (interna o externa) cada dos años a fin de verificar que se cumplen las medidas de seguridad que exige la normativa de protección de datos.

- **Nivel básico:** Es un fichero o tratamiento de datos básico cualquier otro fichero distinto a los indicados que contenga datos de carácter personal.

  Una de las medidas de seguridad de nivel básico (y que, por tanto, debe implantarse en todo tipo de ficheros automatizados) es que se establezca un procedimiento de asignación y distribución de contraseñas y que las contraseñas se cambien, al menos, una vez al año.

Ahora hablando de nuestro proyecto realizado en prácticas, sí que hacemos uso de estos datos, principalmente de nivel básico al almacenar los datos de nuestro clientes y trabajadores para el uso del programa, se trata de una información numérica, podemos decir que la medida de seguridad que hacemos uso para el acceso de estos datos es el uso del usuario y contraseña del cliente.

ORGANISMO

El organismo encargado del cumplimiento de la normativa de protección de datos de carácter personal es el Comité Europeo de Protección de Datos (CEPD). Éste es un organismo de la Unión Europea que está bajo la responsabilidad de que se aplique el Reglamento general de protección de datos (RGPD) desde el 25 de mayo de 2018. El CEPD es un organismo que está compuesto por el representante de cada Autoridad de Protección de Datos (APD) y por el Supervisor Europeo de Protección de Datos.

En España, la Agencia Española de Protección de Datos (AEPD) es el organismo competente para la protección de las personas físicas en lo relativo al tratamiento de datos

personales derivado de la aplicación de cualquier Convenio Internacional en el que sea parte el Reino de España que atribuya a una autoridad nacional de control esa competencia y la representante común de las autoridades de Protección de Datos en el Comité Europeo de Protección de Datos, conforme a lo dispuesto en el artículo 68.4 del Reglamento (UE) 2016/679.

Por lo tanto, la CEPD ayudará a garantizar que el Reglamento de Protección de Datos se aplique de forma coherente en toda la UE y trabajará para garantizar la cooperación efectiva entre las APD.

PARTICIPANTES

RESPONSABLE DEL TRATAMIENTO

El responsable del tratamiento es la persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que sólo o juntamente con otros decida sobre la finalidad, contenido y uso del tratamiento, aunque no lo realizase materialmente. Sus deberes son llevar un registro de los tratamientos de datos personales que se realizan y atender las peticiones de los ciudadanos sobre las consultas relacionadas con el ejercicio de sus derechos. Además de las relacionadas con la seguridad de los datos.

Actualmente, el responsable del tratamiento se regula en el art.4 del RGPD. Es el responsable de la protección y el control de todos los datos personales que se encuentran en posesión de una empresa o entidad. Le corresponde establecer las finalidades para los que se utilizan los datos personales y qué protección de privacidad debe implementarse. Es el responsable de recoger los datos personales y de determinar la base legal para hacerlo. También determina por cuánto tiempo retener los datos.

El responsable del tratamiento deberá:

1. Incorporar las medidas técnicas y organizativas apropiadas para garantizar el procesamiento legal de datos personales.

2. Aplicar políticas adecuadas de protección de datos.

3. Llevar a cabo una evaluación de impacto de privacidad cuando sea necesario.

4. Adherirse a los códigos de conducta elaborados por las autoridades de supervisión en los Estados miembros.

5. Considerar la protección de datos por diseño y por defecto en las actividades de procesamiento.
6. Demostrar el cumplimiento del Reglamento.

En el caso en el que las obligaciones previamente dichas no se cumplan, la infracción será considerada grave, con una multa administrativa de 10.000.000 de euros como máximo y si es empresa el 2% como máximo del volumen de negocio total anual global del ejercicio financiero anterior.

INTERESADO/A

Según la RGPD, el interesado es el titular de los datos o la persona concernida por los datos. Toda información sobre una persona física identificada o identificable («el interesado»), se considera mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona.

Es uno de los principios de la protección de datos según el RGPD. El consentimiento del interesado, atendiendo a lo que enuncia el RGPD, se trata de una comunicación libre por parte del interesado por la cual acepta que se traten sus datos, para una finalidad concreta, bajo unas determinadas condiciones, de las cuales tiene que estar previamente informado.

Por lo tanto, se observan 4 características que debe contar el consentimiento para ser lícito:

- **Libre**: El consentimiento tiene que ser prestado en un marco de libertad. La concesión del mismo no puede estar condicionado a, por ejemplo, una rebaja en un servicio, consecución de un producto, o a cualquier otro tipo de condición.

- **Específico:** Con esto el regulador quiere asegurarse que cuando el tratamiento tenga varias finalidades se recabe el consentimiento para cada uno de ellos. Por ejemplo, si la finalidad con la que se recogen se define como «tratamiento de los datos para la prestación de un servicio», no podrán ser usados para otra finalidad, como por ejemplo elaboración de bases de datos con fines de marketing.

- **Informado:** Se deberá comunicar al interesado de:

    - la finalidad del tratamiento para el que se quiere recabar el consentimiento
    - el nombre del responsable del tratamiento
    - cómo se van a tratar esos datos
    - los derechos de los que es titular el interesado

- **Inequívoco:** La forma de obtención del consentimiento tiene que ser entendible, es decir que el afectado sepa sin lugar a dudas para que está dando su beneplácito. No sería válida que la información sobre la prestación de dicho

consentimiento viniera oculta o mezclada con, por ejemplo, las condiciones de prestación de un servicio.

El RGPD establece una serie de condiciones para legitimar el consentimiento recogido:

- **Demostración:** El responsable del tratamiento deberá ser capaz de demostrar que el interesado consintió el tratamiento de sus datos personales.

- **Distinción:** Si el consentimiento del interesado se da en el contexto de una declaración escrita que también se refiera a otros asuntos, la solicitud de consentimiento se presentará de forma que:
    - se distinga claramente de los demás asuntos
    - de forma inteligible y de fácil acceso
    - utilizando un lenguaje claro y sencillo

- **Revocación:** El interesado deberá poder retirar el consentimiento en cualquier momento. Hay que destacar que la retirada del consentimiento no afectará a la licitud del tratamiento basada en el consentimiento previo a su retirada. Debe ser tan fácil retirar el consentimiento como darlo.

- **Libertad:** Al evaluar si el consentimiento se ha dado libremente, se tendrá en cuenta el hecho de si, entre otras cosas, en la ejecución de un contrato, incluida la prestación de un servicio, se supedita al consentimiento al tratamiento de datos personales que no son necesarios para la ejecución de dicho contrato.

El tratamiento de los datos personales de un menor de edad únicamente podrá fundarse en su consentimiento cuando sea mayor de catorce años. Se exceptúan los supuestos en que la ley exija la asistencia de los titulares de la patria potestad o tutela para la celebración del acto o negocio jurídico en cuyo contexto se recaba el consentimiento para el tratamiento.

El tratamiento de los datos de los menores de catorce años, fundado en el consentimiento, sólo será lícito si consta el del padre/madre/tutor, con el alcance que determinen el padre/madre/tutor

DERECHOS

La normativa de protección de datos permite que puedas ejercitar ante el responsable tus derechos de acceso, rectificación, oposición, supresión ("derecho al olvido"), limitación del tratamiento, portabilidad y no ser objeto de decisiones individualizadas. Estos derechos se caracterizan por lo siguiente:

- Su ejercicio es gratuito.
- Si las solicitudes son manifiestamente infundadas o excesivas (carácter repetitivo) el responsable podrá:
  - Cobrar un canon proporcional a los costes administrativos soportados;
  - Negarse a actuar.
- Deben responderse en el plazo de un mes.
- Se puede prorrogar otros dos meses más, teniendo en cuenta la complejidad y número de solicitudes.
- El responsable está obligado a informarte sobre los medios para ejercitar estos derechos.
- Estos medios deben ser accesibles y no se puede denegar este derecho por el solo motivo de que optes por otro medio.
- Si el responsable no da curso a la solicitud, informará y a más tardar en un mes, de las razones de su no actuación y la posibilidad de reclamar ante una Autoridad de Control.
- Puedes ejercitarlos directamente o por medio de tu representante legal o voluntario.
- Cabe la posibilidad de que, por cuenta del responsable, sea el encargado el que atienda tu solicitud, si ambos lo han establecido en el contrato o acto jurídico que les vincule

Vamos a entrar en más detalles sobre el derecho de limitación y el de portabilidad:

- El derecho a la limitación del tratamiento es el que permite a cualquier interesado, del que se disponen datos personales como objeto de tratamiento, solicitar al responsable del tratamiento que aplique medidas sobre esos datos para, entre otras cosas, evitar su modificación o, en su caso, su borrado o supresión.

Esto significa que los datos de una persona solo pueden ser tratados con su consentimiento para la formulación del ejercicio o la defensa de reclamaciones, con miras a la protección de los derechos de otra persona física o jurídica o por razones de interés público de la UE o de un determinado Estado miembro de la UE. Además, cualquier ciudadano debe ser informado antes del levantamiento de dicha limitación.

Este derecho tiene su antecedente en el derecho al bloqueo previsto en la **Directiva 95/46/CE**. Esta Directiva preveía el derecho del interesado al bloqueo de los datos cuyo tratamiento no se ajuste a las disposiciones de la presente Directiva. En particular a causa del carácter incompleto o inexacto de los datos». Pero fue derogada por el RGPD, cuya aplicación efectiva se produce desde el 25 de mayo de 2018.

En la ley se indican las condiciones que tienen que darse para que el interesado pueda obtener del responsable del tratamiento la limitación del tratamiento de sus datos personales.

Se trata de los casos en los que se procedería el derecho a la limitación del tratamiento.

En segundo lugar, regula el alcance de este derecho y la obligación de información que tiene que facilitar el responsable del tratamiento al interesado.

Con este derecho se permite un mayor control al ciudadano sobre sus datos personales. Y es independiente de los demás derechos que le corresponden. Este derecho también puede facilitar que el interesado pueda denunciar un incumplimiento de la normativa sobre protección de datos. O para, en su caso, presentar ante los tribunales competentes una demanda en caso de que se hayan vulnerados derechos económicos o morales del interesado, es decir, que se haya producido un daño que puede ser objeto de indemnización.

- El derecho a la portabilidad de los datos consiste según el artículo 20 del GRPD, el interesado tendrá derecho a recibir los datos personales que le incumban, que haya facilitado a un responsable del tratamiento, en un formato estructurado, de uso común y lectura mecánica, y a transmitirlos a otro responsable del tratamiento sin que lo impida el responsable al que se los hubiera facilitado. Se trata de un elemento que viene a otorgar un mayor poder de control del interesado sobre sus datos personales, es decir:

  - Posibilidad de conseguir, «en un formato electrónico organizado y comúnmente usado», una copia de los datos que están siendo tratados. Formato que debe permitir que puedan seguir utilizándose por la persona interesada en otro sistema o aplicación informática.

  - Decidir transmitir esos datos a otro sistema (a otro proveedor o prestador de servicios), siempre que los datos objeto de esa trasmisión estén sujetos a un tratamiento automatizado. Para ello también se prevé que estos sean transferidos en un «formato electrónico comúnmente utilizado». Todo ello sin que el responsable del tratamiento ponga obstáculos, impedimentos o dificultades para la cesión de esos datos.

A la hora de solicitar una portabilidad de datos debe contener:

- Identificación: Nombre, apellidos y fotocopia del documento nacional de identidad del interesado o de la persona que lo represente. La fotocopia del documento nacional de identidad podrá ser sustituida siempre que se acredite la identidad por cualquier otro medio válido en derecho
- Petición concretando los datos sobre los que se quiere realizar la portabilidad.
- Identificar el destino de los datos tras la portabilidad.
- Documentación justificativa de la portabilidad solicitada.
- Domicilio a efectos de notificaciones, fecha y firma del solicitante.

En cuanto a nuestro proyecto, sumado a los dos derechos anteriores, los interesados/as tendrían los siguientes derechos:

- **Tu derecho de acceso**

  Supone tu derecho a dirigirte al responsable del tratamiento para conocer si está tratando o no tus datos de carácter personal y, en caso de que se esté realizando dicho tratamiento obtener información sobre:

  - Obtener copia de tus datos personales que son objeto de tratamiento.
  - Los fines del tratamiento.
  - Las categorías de datos personales de que se trate.
  - De ser posible, el plazo previsto de conservación de los datos personales o, si no es posible, los criterios utilizados para determinar este plazo.
  - El derecho a presentar una reclamación ante una autoridad de control.

- **Tu derecho de rectificación**

  El ejercicio de este derecho supone que podrás obtener sin dilación indebida del responsable del tratamiento la rectificación de tus datos personales inexactos. Teniendo en cuenta los fines del tratamiento, tienes derecho a que se completen los datos personales que sean incompletos, inclusive mediante una declaración adicional. En tu solicitud deberás indicar a qué datos te refieres y la corrección que haya que realizar, debiendo acompañar, cuando sea necesario, la documentación justificativa de la inexactitud o carácter incompleto de tus datos.

- **Tu derecho de oposición**

  Este derecho, como su nombre indica, supone que te puedes oponer a que el responsable realice un tratamiento de los datos personales en los siguientes supuestos:

  - Cuando sean objeto de tratamiento basado en una misión de interés público o en el interés legítimo, incluido la elaboración de perfiles. El responsable dejará de tratar los datos salvo que acredite motivos imperiosos que prevalezcan sobre los intereses, derechos y libertades del interesado, o para la formulación, el ejercicio o la defensa de reclamaciones.

  - Cuando el tratamiento tenga como finalidad el "marketing directo", incluida también la elaboración de perfiles anteriormente citada.

    - Ejercitado este derecho para esta finalidad, los datos personales dejarán de ser tratados para dichos fines.

    - Si la campaña publicitaria se realizase, por ejemplo, a través de los datos que posee una empresa contratada, se dará traslado de la petición al anunciante en un plazo máximo de 10 días hábiles.

- **Tu derecho de supresión**

  Podrás ejercitar este derecho ante el responsable solicitando la supresión de sus datos de carácter personal cuando concurra alguna de las siguientes circunstancias:

  - Si tus datos personales ya no son necesarios en relación con los fines para los que fueron recogidos o tratados de otro modo.

  - Si tus datos personales han sido tratados ilícitamente.

  - Si el tratamiento de tus datos personales se ha basado en el consentimiento que prestaste al responsable, y retiras el mismo, siempre que el citado tratamiento no se base en otra causa que lo legitime.

PROCEDIMIENTOS Y DOCUMENTOS

EJERCER DERECHOS

La normativa de protección de datos permite que puedas ejercitar ante el responsable tus distintos tipos de derechos. Dichos derechos se caracterizan por gozar de un ejercicio gratuito. En caso de que las solicitudes sean manifiestamente infundadas o excesivas el responsable podrá cobrar un canon proporcional a los costes administrativos o negarse a actuar.

Deben responderse en el plazo de un mes, pudiéndose prolongar en otros dos meses más, teniendo en cuenta la complejidad y número de solicitudes. El responsable será el encargado de informarte sobre los medios para ejercitar esos derechos. Si el responsable no cumple con sus obligaciones, da razones sobre su no actuación y da la posibilidad de reclamar ante una Autoridad de Control. Se pueden ejercitar los derechos directamente o por medio del correspondiente representante legal o voluntario.

Ahora bien, ciñéndonos a lo que nos concierne, los recursos y procedimientos que los interesados deben seguir para poder ejercitar sus derechos. En primer lugar, la petición debe estar dirigida al responsable que posea los derechos personales. En caso de que el responsable tenga dudas sobre la identidad del interesado, podrá solicitarle información adicional para confirmar la misma. En caso de que se ejerciten a través de un representante, será necesario aportar un documento o instrumento electrónico que acredite esa representación. El interesado deberá presentar una petición en que se concreta la solicitud. También será necesario proporcionar una dirección a efecto de notificaciones, la fecha y la firma del interesado. Además, en caso de que la petición que realice necesite documentos acreditativos, deberán ser presentados también.

En virtud del principio de transparencia recogido en el RGPD, la información que te facilite el responsable, adoptando las medidas oportunas al respecto, debe ser: concisa, transparente inteligible y de fácil acceso con un lenguaje claro y sencillo.

El responsable puede facilitarte la información sobre el tratamiento de tus datos personales puede realizarlo mediante alguno de los siguientes medios:

- Por escrito, por ejemplo, en un formulario en papel
- Por otros medios, incluidos los electrónicos, tales como una página web, etc.
- Verbalmente, siempre y cuando se pueda demostrar la identidad del interesado por otros medios.

La información se te podrá proporcionar junto con iconos normalizados que permitan dar una adecuada visión de conjunto del tratamiento previsto. En este caso, si los iconos se presentan en formato electrónico tendrán que ser «legibles mecánicamente», de manera que el dispositivo que utilices te permita conocer dicha información.

La Comisión Europea podrá determinar la información que se debe presentar a través de los iconos normalizados y los procedimientos aplicables para facilitar dichos iconos.

En cualquier caso, la información sobre el tratamiento de los datos personales tendrá que facilitarte la información de manera gratuita.

SUPRESIÓN

En cuanto a la supresión de datos, la RGPD bajo su artículo 17 regula el derecho que asiste a los titulares de carácter personal, consistente en solicitar a los responsables del tratamiento la supresión de todos aquellos datos de su titularidad. Para que las/os interesadas/os puedan ejercer el derecho de supresión de datos personales, es necesario que se den alguna de las siguientes circunstancias:

- Que los datos personales ya no sean necesarios en relación con los fines para los que fueron recogidos o tratados de otro modo.
- Que el interesado (titular de los datos) retire el consentimiento en que se basaba el tratamiento.
- Que el interesado se oponga al tratamiento y no prevalezcan otros motivos legítimos para el tratamiento,

- Que los datos personales hayan sido tratados ilícitamente.

- Que los datos personales deban suprimirse para el cumplimiento de una obligación legal.

Por otra parte, existe una serie de excepciones que recoge el tercer apartado del artículo 17 del RGPD. Estas excepciones son situaciones en las que el interesado (titular de los datos personales) no podrá ejercer el derecho de supresión siempre y cuando el tratamiento de sus datos por parte del responsable sea necesario para:

- Ejercer el derecho a la libertad de expresión e información.

- El cumplimiento de una obligación legal que requiera el tratamiento de dichos datos, o para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable.

- Por razones de interés público en el ámbito de salud pública.

- Con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, en la medida en que el ejercicio de dicho derecho pudiera hacer imposible u obstaculizar gravemente el logro de los objetivos de dicho tratamiento.

- La formulación, el ejercicio o la defensa de reclamaciones.

EVALUACIÓN DE IMPACTO

La denominada Evaluación de Impacto de Datos Personales (EIPD) consiste en realizar un análisis de los riesgos que la prestación de un servicio puede suponer para la protección de datos personales de los usuarios y, en función de su resultado, marcará la forma en que debemos hacernos cargo de esos riesgos, adoptando las medidas que resulten preceptivas para solventarlos, de forma que podamos garantizar que los datos personales de nuestros clientes sean debidamente protegidos.

En otras palabras, se trata de evaluar el impacto en la protección de datos personales respecto a las opciones que pueden adoptarse en relación con un determinado modelo de negocio.

En función de qué clase de datos y qué volumen de los mismos se manejen, estos análisis requerirán un grado de intensidad muy distinto. Esto se debe a que los riesgos pueden ser mínimos o fácilmente salvables, y por contra en otros casos, pueden hacer necesario implementar acciones más rigurosas debido a la dificultad que tales riesgos plantean.

La finalidad que se persigue al realizar una EIPD es posibilitar que los responsables del tratamiento adopten medidas tendentes a reducir esos riesgos que nos obligan a hacerla (disminuyendo la probabilidad de su materialización y las consecuencias negativas para los usuarios).

Un aspecto para destacar sería que en virtud del nuevo principio denominado del "diseño por defecto", (establecido en el RGPD), las evaluaciones deben realizarse antes de comenzar a realizar el tratamiento de esos datos personales; y por ende debe de practicarse un análisis previo de los riesgos que determine o no su obligatoriedad.

La evaluación de impacto deberá practicarse cuando el tratamiento de los datos personales entrañe un riesgo alto para los derechos y libertades de los usuarios.

En cuanto los puntos que debe contener un informe final de la EIPD podemos destacar los siguientes:

- Una descripción general de las operaciones de tratamiento previstas.
- Una evaluación de los riesgos para los derechos y libertades de los interesados.
- Las medidas contempladas para hacer frente a los riesgos y amenazas.
- Garantías, medidas de seguridad y mecanismos destinados a garantizar la protección de datos personales y a demostrar la conformidad con el reglamento, teniendo en cuenta los derechos e intereses legítimos de los interesados y de otras personas afectadas.

Existen también otros contenidos adicionales que pueden incluirse en el informe de EIPD como:

- Referencia a posibles Códigos de Conducta aplicables (una herramienta muy útil para la autorregulación de sectores de actividad concretos).
- Opinión de los interesados o de sus representantes, sin perjuicio de la protección de intereses públicos o comerciales o la seguridad del tratamiento.

DOCUMENTOS

Para cumplir con la ley vigente, tratándose datos de ámbito personal, los documentos a elaborar que han de cumplir totalmente con el RGPD son los siguientes:

- **Política de Protección de Datos Personales** (Artículo 24): Éste es un documento de alto nivel para la gestión de privacidad de una empresa, que define lo que ésta quiere alcanzar y la manera que utiliza para ello.

- **Aviso de Privacidad** (Artículos 12, 13, y 14): Este documento (que puede ser también publicado en la página web de la empresa) explica en palabras sencillas cómo se tratarán los datos personales de sus clientes, visitantes del sitio web, y otros.

- **Aviso de Privacidad de los Empleados** (Artículos 12, 13 y 14): Explica cómo la empresa va a tratar datos personales de sus empleados (que pueden incluir registros de salud, antecedentes penales, etc.)

- **Política de Retención de Datos** (Artículos 5, 13, 17, y 30): Describe el proceso de decidir cuánto tiempo va a guardarse un tipo de datos personales en particular, y cómo se destruirá posteriormente de forma segura.

- **Programa de Retención de Datos** (Artículo 30): Enumera todos los datos personales y describe cuánto tiempo se conservará cada tipo de datos.

- **Formulario de Consentimiento del Interesado** (Artículos 6, 7, y 9): Ésta es la forma más común de obtener el consentimiento de un interesado/a para tratar sus datos personales. Este documento está bajo seis bases jurídicas para tratamiento de datos de acuerdo al RGPD (Obligaciones de ley y cumplimiento legal, Rendimiento contractual, Intereses vitales, Interés público o actuación bajo autoridad pública oficial, Intereses legítimos y Consentimiento de los interesados).

- **Formulario de Consentimiento Paterno** (Artículo 8): Si el interesado tiene menos de 16 años, entonces el padre necesita proporcionar el consentimiento para tratar los datos personales.

- **Registro de EIPD** (Artículo 35): Aquí es donde registra todos los resultados de la Evaluación de Impacto de Protección de Datos.

- **Acuerdo de Tratamiento de Datos del Proveedor** (Artículos 28, 32, y 82): Se necesita este documento para regular la protección de datos con un encargado de tratamiento o cualquier otro proveedor.

- **Procedimiento de Respuesta a la Violación de Seguridad de Datos** (Artículos 4, 33, y 34): Describe qué hacer antes, durante y después de una violación de seguridad de datos.

- **Registro de Violación de Seguridad de Datos** (Artículo 33): Aquí es donde se registrará todas las violaciones de seguridad de datos.

- **Formulario de Notificación de Violación de Seguridad de Datos a la Autoridad de Control** (Artículo 33): En caso de tener una violación de seguridad de datos, tendrá que notificarlo formalmente a la Autoridad de Control.

- **Formulario de Notificación de Violación de Seguridad de Datos a los Interesados** (Artículo 34): En caso de una violación de seguridad de datos, tendrá la desagradable obligación de notificar a los interesados de manera formal.

Por otra parte, existen ciertos documentos que son necesarios bajo ciertas condiciones, los cuales son los siguientes:

- **Descripción del Puesto de Delegado de Protección de Datos** (Artículos 37, 38, y 39): Es necesario disponer de un Delegado de Protección de Datos (DPD) si:
  - a) El tratamiento es llevado a cabo bajo una autoridad u organismo público, a excepción de los tribunales que actúan en su capacidad judicial.
  - b) Las actividades centrales consisten en operaciones de tratamiento que precisan un seguimiento regular y sistemático de los interesados a gran escala.
  - c) Las actividades centrales tratan una categoría especial a gran escala de datos y datos personales relacionados con condenas y delitos penales.

- **Listado de Actividades de Tratamiento** (Artículo 30): Este documento es obligatorio si:
  - a) La empresa tiene más de 250 empleados.
  - b) El tratamiento que lleva a cabo la empresa puede resultar un riesgo para los derechos y libertades de los interesados.
  - c) El tratamiento no es ocasional.
  - d) El tratamiento incluye categorías especiales de datos.
  - e) El tratamiento incluye datos personales relacionados con condenas y delitos penales.

- **Cláusulas Contractuales Estándar para la Transferencia de Datos Personales a Responsables** (Artículo 46): Obligatorio si transfiere datos personales a un *responsable* fuera del Área Económica Europea (AEE) y se ampara en cláusulas modelo como la base legal para las transferencias transfronterizas de datos.

- **Cláusulas Contractuales Estándar para la Transferencia de Datos Personales a Encargados** (Artículo 46): Obligatorio si transfiere datos personales a un *encargado* fuera del Área Económica Europea (AEE) y se ampara en cláusulas modelo como la base legal para las transferencias transfronterizas de datos.

OBLIGACIONES Y SANCIONES

OBLIGACIONES

Con la LOPD 15/1999 y su Reglamento de Desarrollo 1720/2007 se implantaban medidas de seguridad taxativas, que regulaban al detalle qué concretas medidas debían establecer las organizaciones para salvaguardar sus datos de carácter personal.

Las medidas de seguridad vienen recogidas en el art. 80 RLOPD, y se dividen en tres niveles: básico, medio y alto.

Para cada uno de estos niveles, se aplicaban distintas medidas de seguridad en función del tipo de datos objeto del tratamiento y de la necesidad de una mayor o menor confidencialidad e integridad de la información.

A modo de ejemplo, se puede considerar:

- Nivel Básico: Nombre y apellidos, número de teléfono, DNI, etc.
- Nivel Medio: Datos relativos a solvencia patrimonial y crédito, curriculums, sanciones administrativas, etc.
- Nivel Alto: Datos relativos a la salud, afiliación sindical, ideología, origen racial o étnico, etc.

Estas medidas eran acumulativas, de manera que cuando un fichero tuviera un tratamiento con un nivel de seguridad Medio, se debían implantar las medidas del Nivel Básico y las del Medio. Todas estas medidas debían aparecer reflejadas en el Documento de Seguridad de la organización, siendo requisito imprescindible, su redacción por el responsable del Fichero.

Sin embargo, dicho documento no existe con el Reglamento Europeo de Protección de Datos 2016/679 (UE) (RGPD), ya que se da un giro de tuerca a esta situación, debido a la instauración de dos Principios clave: el Principio de Accountability y el Principio de Enfoque al Riesgo.

En función del Principio de Accountability o Responsabilidad Proactiva, el responsable del Tratamiento debe aplicar las medidas técnicas y organizativas necesarias a fin de garantizar y poder demostrar que cumple con el RGPD. Este principio exige una actitud proactiva y diligente por parte de las organizaciones, que tienen que ser capaces de demostrar, tanto ante las autoridades como ante los interesados, que las medidas implantadas son las adecuadas para cumplir con el RGPD.

El nuevo Reglamento Europeo de Protección de Datos, para ayudar al Responsable y/o Encargado de Tratamiento en su tarea de analizar y determinar cuáles son las medidas adecuadas a implantar por su empresa, prevé la adhesión a códigos de conducta aprobados, certificaciones aprobadas, seguimiento de directrices dadas por el Comité Europeo de Protección de Datos (CEPD) o indicaciones proporcionadas por un Delegado de Protección de Datos, como mecanismo para garantizar y poder demostrar que su organización cumple con el nuevo Reglamento.

Por otro lado, el Principio de Enfoque al Riesgo, supone que las organizaciones antes de implantar cualquier tipo de medidas 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. La aplicación de este principio implica que las empresas deberán analizar de manera previa al tratamiento: si existe un alto riesgo para los derechos y libertades de los

ciudadanos y cómo deben modularse las medidas en función del tipo de riesgo y de las características de las organizaciones.

Para la realización del análisis de riesgos se debe tener en cuenta:

- El número de interesados.
- La naturaleza de los datos.
- El número de tratamientos.
- Variedad de tratamientos que una misma empresa efectúe.

Ambos principios, constituyen una de las novedades más importantes que incluye el RGPD en la medida en que sobre ellos pivota el conjunto de medidas técnicas y organizativas que deben adoptar las empresas para el almacenamiento, seguimiento y adecuada protección y seguridad de los datos de carácter personal.

SANCIONES

El Reglamento europeo de Protección de Datos únicamente regula criterios o cuestiones básicas en relación con las infracciones y sanciones. En cuanto a la hora de aplicar estas sanciones, se deben tener en cuenta diferentes aspectos:

Personal competente para la investigación por incumplimiento de RGPD:

- Funcionarios de la Agencia
- Funcionarios externos que hayan sido previamente habilitados por el director de la AEPD

En caso de cometerse una infracción en relación con la protección de datos, se consideran sujetos responsables:

- Responsables del tratamiento
- Encargados del tratamiento
- Representantes de los responsables o encargados de los tratamientos no establecidos en la Unión Europea
- Entidades de certificación
- Entidades acreditadas de supervisión de los códigos de conducta (AEPD)
- Autoridades de control

Es importante mencionar que la figura del delegado de protección de datos no podrá ser sancionado como sujeto responsable.

En cuanto a las infracciones, el RGPD recoge dos tipos de infracciones:

Infracciones graves:

Estas infracciones prescriben a los dos años. Serán sancionadas con multas administrativas de 10.000.000 de euros como máximo, y si es empresa el 2% como máximo del volumen de negocio total anual global del ejercicio financiero anterior.

Las infracciones consideradas como graves se darán en los casos donde no se cumplan:

- Obligaciones del responsable y del encargado
- Los compromisos de los organismos de certificación
- Obligaciones de la autoridad de control

Infracciones muy graves:
En este caso, prescriben a los tres años. Serán sancionadas con multas administrativas de hasta 20.000.000 de euros, y si es empresa una cuantía equivalente a un máximo del 4% del volumen de negocio total anual global del ejercicio financiero anterior.

La calificación de las infracciones como muy graves se darán en los supuestos donde no se cumplan:

- Los principios básicos para el tratamiento, incluido el consentimiento.
- Los derechos de los interesados de acceso, rectificación, cancelación, oposición, limitación y portabilidad.
- Requisitos establecidos para realizar transferencias de datos personales a un destinatario en un tercer país o una organización internacional.
- Las obligaciones que adopten los Estados miembros.
- Una resolución o limitación temporal o definitiva del tratamiento o la suspensión de los flujos de datos por parte de la autoridad de control.

Procedamos ahora a explicar el procedimiento sancionador ante una infracción.

El inicio de este procedimiento puede producirse o bien por no atender la solicitud del ejercicio de los derechos del interesado o cuando pueda existir una infracción del reglamento. En caso de que, por ejemplo, las reclamaciones no tengan nada que ver con cuestiones de protección de datos de carácter personal, carezcan manifiestamente de fundamento, sean abusivas, etc., no serán admitidas de ninguna manera. Independientemente de ser admitidas o no, esta resolución debe notificarse en un plazo de 3 meses. En caso de no haber una comunicación en dicho plazo, se sobreentiende como admitida y continúa el procedimiento.

Puede existir una fase previa de alegaciones para la investigación una vez que se haya admitido la reclamación con el fin de determinar la situación. Finalizada la fase de alegaciones previas, el director de la AEPD dictará cuando sea necesario, el acuerdo del inicio del procedimiento donde se reflejarán los hechos, la identificación de la persona o entidad contra la que se dirija el procedimiento, la posible infracción y su posible sanción.

La AEPD podrá llevar a cabo actuaciones de inspección a fin de lograr una mejor determinación de los hechos y las circunstancias que justifican la tramitación del procedimiento. No podrá durar más de 12 meses a contar desde la fecha de admisión. En el ejercicio de las actividades de investigación pertinentes, los funcionarios de la AEPD pueden:

- Recabar la información precisa para el cumplimiento de sus funciones
- Realizar inspecciones
- Solicitar el envío de documentos o datos necesarios
- Examinar, obtener copias e inspeccionar los equipos
- Requerir la ejecución de tratamientos y programas sujetos a la investigación

BIBLIOGRAFÍA

https://ayudaleyprotecciondatos.es/2018/11/09/derecho-limitacion-rgpd/#Que_es_el_derecho_a_la_limitacion_del_tratamiento_de_datos

https://ec.europa.eu/info/law/law-topic/data-protection/reform/rights-citizens/my-rights/when-should-i-exercise-my-right-restriction-processing-my-personal-data_es

https://ayudaleyprotecciondatos.es/2019/02/20/evaluacion-impacto-proteccion-datos-rgpd/

https://www.aepd.es/media/guias/guia-ciudadano.pdf

https://www.iberley.es/temas/glosario-definiciones-rgpd-62717

https://protecciondatos-lopd.com/empresas/datos-especialmente-protegidos-sensibles/

https://www.aepd.es/media/guias/guia-rgpd-para-responsables-de-tratamiento.pdf

https://ayudaleyprotecciondatos.es/2018/11/12/derecho-informacion-rgpd/

https://protecciondatos-lopd.com/empresas/procedimiento-sancionador-rgpd/#Sanciones_por_incumplimiento_de_RGPD

Real Decreto 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia de Protección de Datos. *Boletín Oficial del Estado, 106,* 4 de mayo de 1993.

Advisera Expert Solutions Ltd. Base de conocimientos RGPD UE

Agencia Española Protección Datos (AEPD). Ejerce tus derechos.

Iberley. Derecho de supresión (borrado de datos) y derecho al olvido en la LO 3/2018 (LOPDGDD) y en el Reglamento General de Protección de Datos (RGPD).

Grupo Adaptalia. El derecho de supresión en el RGPD.

https://blog.binapsys.com/rgpd-definiciones/

http://guiasjuridicas.wolterskluwer.es/Content/Documento.aspx?params=H4sIAAAAAAAEAMtMSbF1jTAAAkNjEwMjE7Wy1KLizPw8WyMDQwsDU0OwQGZapUt-ckhlQaptWmJOcSoAQPEJJDUAAAA=WKE