EIPD

¿Qué es una EIPD? ¿Qué necesidad hay de realizarla?

Una vez tenemos claro que vamos a hacer con los datos, de que tipo son los datos, que futuro les espera en nuestra empresa o fuera (cesión, transferencias internacionales) llega el momento de estudiar su seguridad.

En todo momento debemos conjugar las necesidades que tiene nuestra empresa de ellos con los derechos del interesado, lo que nos llega, como ya sabemos, a la confección del registro de actividades de tratamiento donde disponemos de una visión categorizada de los mismos. Esto es un paso previo e imprescindible para poder afrontar una EIPD, sin una visión clara y completa donde se contemplen los derechos de los interesados, no podemos buscar los problemas, tanto responsables y encargados irán perdidos sin saber analizar su naturaleza y alcance, al tenerlo descontextualizado y desconociendo su finalidad.

Con el EIPD tratamos de anticiparnos y evaluar los (al menos) principales riesgos que pueden llegar a presentarse que afecten a los datos personales que custodiamos para realizar las actividades de tratamiento de nuestra organización. Hablamos de palabras más conocidas para nosotros como la expresión "análisis de riesgos", "amenazas", "resiliencia", etc. El trabajo del especialista aquí pasa por diseñar e implementar aquellas medidas de seguridad y control precisas considerando que el EIPD es una herramienta preventiva.

El EIPD tiene como objetivo la identificación, evaluación y gestión constante de los riesgos de las actividades de tratamiento de una entidad y siempre es previa al inicio de las mismas.

¿Y si tenemos ya en marcha tratamientos, de forma previa a la entrada en vigor a la norma? Sobre el papel solo nos afectaría sin introducimos elementos nuevos (p.e. perfilado) o finalidades distintas en el tratamiento, pero es una buena praxis realizarla de todas formas.

¿Y si uno de esos antiguos tratamientos, al realizar la EIPD vemos que tienen grandes riesgos? Sencillo. O anulamos los riesgos… o anulamos el tratamiento.

El análisis previo

Aquí debemos diferenciar aquellos tratamientos donde es obligado hacer una EIPD y aquellos donde no. De todas formas, siempre es conveniente realizarla, pero pondremos primero el acento en aquellos donde es imprescindible por ser supuestos de obligada realización (art. 35.3 RGPD). Hay tres casos que nos marca el reglamento:

- Cuando se produzca una evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas físicas o que les afecten significativamente de modo similar. *Ojo: ese tratamiento automatizado, la generación de perfiles, no depende de las categorías de datos que son tratados*.
- Cuando exista un tratamiento a gran escala de las categorías especiales de datos o de datos personales relativos a condenas e infracciones penales. *Aquí cabría preguntarnos por el*

*concepto de "*gran *escala", pues podemos pensar en grande por extensión geográfica (más de un país) o por elevada cantidad de interesados. Cualquiera de estas dos condiciones nos vale. Ejemplos típicos serían aseguradoras médicas, hospitales, abogados penalistas, etc., que sean parte de grandes corporaciones o tengan un gran número de usuarios. Una clínica dental particular, no sería un elemento típico de este criterio.*

- Cuando se proceda a la observación sistemática a gran escala de una zona de acceso público. *Se nuevo aparece la idea de "gran escala", pero aparece la "observación", ligada a los sistemas de videovigilancia. En general no es posible colocar cámaras en espacios públicos, pero existen excepciones, como cuando es imprescindible para la salvaguarda de bienes, derechos o la propia instalación o por ser trata instalaciones o infraestructuras estratégicas o relacionadas con el transporte público. Ojo porque acceso público no siempre es igual a zona pública, en una propiedad privada puede existir un acceso público (clientes en un centro comercial).*

Ya tenemos claro donde hay que hacer, en cualquier caso, una EIPD. Vamos ahora como los supuestos donde es recomendable hacerla. (art. 35.1 RGPD).

> *Cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento realizará, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales. Una única evaluación podrá abordar una serie de operaciones de tratamiento similares que entrañen altos riesgos similares.*

Para este punto es imprescindible una consulta a la web de la AEPD y la descarga de su "Guía Práctica de análisis de riesgos en los tratamientos de datos personales sujetos al RGPD[1]". Con su ayuda analizamos los factores clave del artículo del RGPD. De hecho lo que sigue es casi una copia literal de ese documento.

Naturaleza del tratamiento: se valoran las características más básicas del tratamiento y ver si estas pueden implicar un alto riesgo, respondiendo a preguntas como

- ¿Se tratan categorías especiales de datos?
- ¿Se tratan datos a gran escala?
- ¿Se hace un seguimiento exhaustivo de las personas?
- ¿Se combinan diferentes conjuntos de datos? (fuentes de información diferentes)
- ¿Los datos se refieren a personas en situación de vulnerabilidad? (menores de 14 años o discapacitados, p.e.)

Alcance del tratamiento: se valoran los efectos o consecuencias del tratamiento, identificando hasta qué punto puede llegar y si éste puede suponer un alto riesgo, respondiendo a preguntas como

- ¿Se realiza un proceso de toma de decisiones con efectos jurídicos?
- ¿Se realiza una valoración de riesgo crediticio?
- ¿Se valora la exclusión de beneficios sociales o fiscales?

[1] Disponible en: https://www.aepd.es/sites/default/files/2019-09/guia-analisis-de-riesgos-rgpd.pdf (Consultado el 29 de julio de 2020)

Contexto del tratamiento: se valoran el conjunto de circunstancias bajo las cuales se realizarán las actividades de tratamiento, con el objetivo de verificar si pueden suponer un alto riesgo, respondiendo a preguntas como:

- ¿Se realiza un uso de nuevas tecnológicas? ¿son especialmente invasivas para la privacidad?
- ¿Existen varios responsables del tratamiento?
- ¿Existen cadenas complejas de encargados de tratamiento?
- ¿Se producen transferencias internacionales?
- ¿Existen cesiones de datos?

Finalidades del tratamiento: se identifican cada una de las finalidades del tratamiento y analiza si estas derivan en un alto riesgo. Se comprueba p.e. si la finalidad incluye:

- Toma de decisiones
- Elaboración de perfiles
- Análisis predictivo
- Prestación de servicios relacionados con la salud
- Seguimiento, control y observación de personas (monitorización)

La mayoría de las pequeñas y medianas empresas no tendrán que realizar este procedimiento.

Si se está obligado, estará en la órbita del responsable de (los) tratamiento(s) y, si no lo está, decidirá si hacerla o no en función de los condicionantes y evidencias prácticas de que disponga.

Análisis de riesgos

¿Hacemos finalmente una EIPD? ¿No la hacemos? En todo caso es muy recomendable, aunque no la hagamos, llevar a cabo un análisis de riesgos de amplio horizonte, que considere toda amenaza que gravite sobre la entidad y particularmente sobre sus tratamientos.

No, no hay dos análisis de riesgos iguales, de igual forma que no hay dos organizaciones iguales. Cada una tendrá su tamaño, su alcance, su volumen de datos… debemos empezar pues por poner un poco de orden, partiendo del ciclo de vida de los datos (el corazón de los tratamientos que vamos a efectuar). Esto es: vamos a generar un informe en donde aparezcan las fases de vida de aquellas categorías de datos personales que podamos tratar. Desde que nace hasta que muere. O, en nuestro caso, desde que un usuario, un paciente, un cliente, rellena un formulario, hasta que una destructora de documentos y discos duros convierte en partículas los medios que los almacenan.

Pintado con líneas gruesas, podríamos describirlo con la imagen siguiente, en cuatro etapas. Aunque, como veremos, algunas de ellas podrían desdoblarse en subetapas y, para poder tener una visión general, tendremos que considerar todos aquellos agentes externos implicados en cada uno de los procesos.

1. Captura: del interesado a nuestro sistema. Hay muchas vías para poder obtener esta información, sin ánimo de completitud hablaremos de :
    a. Nos lo da el usuario, a través de un formulario (donde irá el consentimiento, e incluso puede ser todo él un documento que enumere todo lo que es relativo al mismo) o de forma oral, o nos lo manda en un correo electrónico, o mediante mensajería (telegram, whatsapp…)
    b. A través de una web
    c. De nuestros archivos (ya lo teníamos de forma previa a la norma: hay que verificar su consentimiento y solicitarlo caso de que no lo tengamos, o si lo tenemos no respete la norma actual)
    d. Del estado, de un ayuntamiento, de… de un organismo público
    e. Nos llega de otra entidad (cesión, p.e.)
2. Almacenamiento de los datos. Dado que tendremos que organizarlo por categorías, el primer paso será la clasificación de los datos
    a. Clasificación: para que nos resulte más cómodo estructurarlos y organizarlos. Podemos seguir el consejo del antiguo reglamento de la LOPD (la ley del 99 que fue antecesora de la actual) y emplear esta clasificación:
        i. Sensibles: los que la norma define como categorías especiales de datos (datos de salud o datos que revelen ideología o creencias). Podríamos incluso hacer un apartado de “ultrasensibles” para hablar de otros que la norma actual no referenciaba, como los datos genéticos.
        ii. Protegidos: datos económicos, solvencia patrimonial, datos no sensibles de discapacitados o menores
        iii. Básicos: en los que solemos pensar cuando hablamos de datos personales: conjunto de datos identificativos de un interesado que no revelan circunstancias relevantes. (nombre, domicilio, DNI...)
    b. Almacenamiento en sí: también de una forma con trazo grueso podríamos hablar de tres subclasificaciones:

i. Papel (carpetas, p.e.)[2]
ii. Digital: para poder verlos nos hace falta un dispositivo. Si se trata de un Telegram con los datos de un cliente y lo imprimimos, tenemos que jugar con las medidas de seguridad de ambas categorías. Advirtamos que en este momento no hacemos distinción alguna a si el fichero lo tenemos en nuestro ordenador de sobremesa o en la nube.
iii. Ambos (mixto): como el ejemplo que acabamos de mencionar.

3. Tratamiento. En este punto del ciclo de vida tendremos que valorar no solo que hacemos con los datos son quienes participan: que elementos se empelan y si lo datos salen de la empresa (p.e. mediante una cesión). Vamos a verlo como partes separadas.
    a. ¿Qué elementos/personas participan en el tratamiento?
        i. Hardware/Software:
            1. portátiles, sobremesa, máquinas virtuales, tabletas…
            2. soportes: papel, discos, duros, tarjetas de memoria externa, la nube…
            3. Software de uso general: ofimática, mensajería, copias de seguridad
            4. Software específico para el tratamiento
        ii. Personas: categorías de personas en la organización que pueden ir desde usuarios internos y usuarios externos a personal subcontratado
        iii. Interesados/afectados: también por categorías (pacientes, familiares de pacientes, clientes, voluntarios de una ONG…)
    b. Operaciones con los datos: no es difícil ver que esta será el corazón del informe. Aquí debemos indicar toda operación concreta se realizará con los datos (financiación de deudas, tratamientos sanitarios, contabilidad…). Es de interés mencionar aquí si se hacen o no perfiles de datos.
    c. Cesiones o transferencias internacionales: ¿vamos a hacer algo de esto? Es el momento de reseñarlo. Si se va a hacer, hay que indicar el tipo de empresa, organización al que serán cedido y/o a que país al que serán transferidos.
4. Destrucción de los datos: en este caso, más importante que el cómo (que no deja de tener su importancia) prima el cuándo:
    a. Tras el plazo legal establecido: lo que diga la ley (p.e. documentación contable)
    b. Por petición expresa del interesado: solo cuando la destrucción estuviese subordinada a esa petición. Serán típicamente datos básicos
    c. En plazo distinto del legalmente establecido, pero determinado previamente: podemos informar al interesado del plazo concreto, pero esto vale solo para los datos que no tengan un plazo legal obligatorio de conservación o que no suponga un incumplimiento de dicho plazo.

¿Qué consideramos en este contexto una amenaza?

Sin querer mostrar un rigor excesivo, podemos hablar de aquellos aspectos que puedan afectar a la privacidad de los interesados y van ligadas a las operaciones de tratamiento. LA AEPD nos sugiere un profundo proceso de identificación, evaluación y tratamiento. Para adentrarse en éste camino, lo podemos más que partir de un conocimiento exhaustivo de la entidad responsable y su contexto, en el que englobamos al personal –incluida la dirección- y sus objetivos. Si quien debe realizar esto no tiene esa información no se podrán identificar todas las amenazas posibles. Insistamos en algo que ya hemos

[2] Aquí te disparo una pregunta: ¿el listado de reparto que lleva un transportista, entra en ésta categoría?

dejado dicho antes: no todas las organizaciones son iguales. No todas tendrán un mismo nivel del riesgo, no todas hacen los mismos tratamientos, emplean el mismo hardware, el mismo software.

Vamos a identificar las amenazas y, una vez identificadas y documentadas, las clasificaremos según los consejos de la AEPD en tipología y gravedad para, por último, poder asignar a cada una, una medida de seguridad que sirva para inhibir al máximo posible la materialización del riesgo. Al máximo posible ya sabemos que muchas veces no significará dejar en cero. De hecho, nunca hablaremos de un riesgo cero como algo tangible.

Un nuevo considerando: de momento aun hablamos solo de esas organizaciones en las que no se aprecie un elevado número de amenazas, o, si estas existen, no afectan a tratamientos de alta sensibilidad o de información especialmente protegida. Si se detecta un alto riesgo, podemos directamente plantearnos una EIPD donde valoraremos tanto el riesgo inherente como el residual a la hora de determinar las medidas de seguridad adecuadas.

Vamos a la guía de la AEPD, en su página 32, para dejar esto claro con un ejemplo.

Actividad de tratamiento: *Registro y almacenamiento de una lista de asistentes a un curso de formación en una aplicación sin elevado riesgo para los derechos y libertades de los interesados.*

Principales riesgos potenciales identificados [3]

1. *Protección de la información:*
    a. *Integridad de los datos personales:*
        i. *Modificación o alteración de datos personales no intencionada*
    b. *Disponibilidad de los datos personales:*
        i. *Pérdida o borrado no intencionado de datos personales*
    c. *Confidencialidad de los datos personales:*
        i. *Acceso no autorizado a los datos personales*
2. *Riesgos asociados al cumplimiento:*
    a. *Garantizar el ejercicio de los derechos de los interesados:*
        i. *Ausencia de procedimientos para el ejercicio de derechos*
    b. *Garantizar los principios relativos al tratamiento:*
        i. *Ausencia de legitimidad para el tratamiento de los datos personales*
        ii. *Tratamiento ilícito de datos personales*

Ejemplos de medidas de control que ayudan a reducir el nivel de exposición del riesgo potencial identificado

Tipología de riesgo	***Riesgo***	***Medidas de control***
Integridad de los datos personales	*Modificación o alteración de datos personales no intencionada*	*Segregación de funciones mediante perfiles de acceso* *Controles de monitorización de amenazas en red*

[3] *Listado de riesgos asociados al cumplimiento normativo disponible en la sección de publicaciones de la web de la AEPD.*

Disponibilidad de los datos personales	*Pérdida o borrado no intencionado de datos personales*	*Copias de seguridad* *Almacenamiento en dos ubicaciones diferentes*
Confidencialidad de los datos personales	*Acceso no autorizado a los datos personales*	*Mecanismos de control de acceso* *Segmentación de la red*

Riesgo

Aún no hemos empezado una EIPD. Todo el análisis previo que hemos visto no es más que un paso necesario, o, si lo queremos ver así, la "parte cero" de la misma. Si debemos realizar la EIPD, nuestra meta a cubrir es determinar y cuantificar la proporción de riesgo inherente del (los) tratamiento(s).

Este paso previo es imprescindible, porque de otro modo no podremos implantar medidas de seguridad proporcionales y adecuadas.

Aunque en otras materias se ha presentado el riesgo, vamos a darle una vuelta más aquí, para verlo desde nuestro punto de vista.

La guía de la AEPD "Guía práctica para las Evaluaciones de Impacto en la Protección de los datos sujetas al RGPD"[4]

> *El riesgo inherente es el riesgo intrínseco de cada actividad, sin tener en cuenta las medidas de control que mitigan o reducen su nivel de exposición. El riesgo inherente surge de la exposición que se tenga a la operación de tratamiento en particular y de la probabilidad de que la amenaza asociada al riesgo se materialice.*

Esto es: aquel que hace referencia al nivel de amenaza que existe de modo intrínseco a la propia figura del responsable según su actividad, organización, estructura y planteamiento de cumplimiento. Hablamos de las amenazas en la organización sin aplicar medida de seguridad alguna. Subrayemos que estamos hablando de riesgo inherente.

Para calcular ese riesgo consideramos dos factores: la probabilidad de que se materialice y el impacto, esto es, las consecuencias en caso de que se acabase materializando.

Riesgo = Probabilidad x Impacto

¿De dónde sacamos la probabilidad? Este es un dato teórico, considerando el contexto de la organización y la amenaza en sí. Volveremos a esto un poco más adelante.

Aun así, nos movemos en un camino de incertidumbre. ¿Cómo afrontamos esto? En ocasiones recurriremos a elementos cualitativos, empleando descripciones, en otras, serán datos, números, atendiendo a escalas cuantitativas y, las más de las veces, tendremos que hacer uso tanto de unas como de otras, con la dificultad evidente de operar al tiempo con peras y con manzanas, con elementos que no pueden sumarse entre sí.

[4] Disponible en https://www.aepd.es/sites/default/files/2019-09/guia-evaluaciones-de-impacto-rgpd.pdf (consulta 30 de julio de 2020)

En todo caso, conviene hacer una consideración previa: a más compleja sea la escala tenemos un efecto positivo, y es el tener mejor definición final de los resultados, pero tambiñen un efecto perverso: el que complica su empleo hasta el extremo de hacerlo inviable, por ejemplo, para pequeñas empresas sin personal humano ni técnicas suficientes. Una solución típica es reducirlo todo a una escala, donde mi propuesta particular es emplear una típica escala Likert de cinco niveles, adaptada para este caso:

0- Imposible. Es un riesgo que existe, pero no afecta a mi organización
1- Improbable: Pude darse, pero se trata de un escenario de riesgo muy remoto para mi organización
2- Probable: No se trata de elementos comunes, pero pueden estar presentes, incluso podemos prever su frecuencia de aparición
3- Muy probable: Son escenarios de riesgo habituales en la empresa
4- Seguros: Pasaremos por eso. Solo queda protegernos de la mejor de las maneras.

La AEPD sugiere una escala muy similar, pero limitando su visión a la parte media de la tabla. Su propuesta es hablar de probabilidades despreciables, limitadas, significativas y máximas. ¿Qué diferencia hay? En la práctica, ninguna, pues los elementos donde la probabilidad se reduce a 0 o se sitúa en el 100%, quedan cubiertos, pero creo que su consideración teórica ofrece una mejor mesa de trabajo para el profesional.

La otra variable a considerar es el impacto. Para él, nos ceñiremos a lo que indica la agencia, que habla también de la escala despreciable – limitada – significativa – máxima.

- Despreciable: un impacto sería despreciable si no tuviera consecuencias sobre el interesado.
- Limitado: Tan solo tiene consecuencias de tipo residual en el interesado.
- Significativo: si el daño ocasionado sobre los derechos y libertades del interesado fuese crítico.
- Máximo: cuando va unido a consecuencias críticas sobre los derechos.

Ya tenemos los dos factores de la ecuación. Así, simplemente multiplicando, podemos dar un peso a ese riesgo. En la siguiente tabla, según el modelo de la AEPD podemos ver los pesos.

Probabilidad	Máximo (4)	4x1 = 4	4x2 = 8	4x3 = 12	4x4 = 8
	Significativo (3)	3x1 = 3	3x2 = 6	3x3 = 9	3x4 = 12
	Limitado (2)	2x1 = 2	2x2 = 4	2x3 = 6	2x4 = 8
	Despreciable(1)	1x1 = 1	1x2 = 2	1x3 = 3	1x4 = 4
		Despreciable(1)	Limitado (2)	Significativo (3)	Máximo (4)
	Impacto				

Lo siguiente es identificar cuatro niveles de riesgo: bajo, medio, alto o muy alto, que ya se pueden asignar a números concretos. Así, con valores de 2 o inferiores, lo consideramos bajo, hasta seis medio, hasta doce alto y mayores de 12, muy altos. Con esto nos quedaría la tabla que nos presenta la AEPD:

Probabilidad	Máximo				
	Significativo				
	Limitado				
	Despreciable				

		Despreciable	Limitado	Significativo	Máximo
	Impacto				

Y ya que estamos hablando de riesgos, vamos con un concepto que la AEPD señala en sus guías: el riesgo residual (y su cálculo).

> *El riesgo residual es el riesgo de cada actividad una vez se hayan aplicado las medidas de control para mitigar y/o reducir su nivel de exposición. A diferencia del riesgo inherente, el riesgo residual contempla las medidas de control definidas sobre la actividad de tratamiento para valorar la probabilidad y/o el impacto asociado al riesgo.*

Emplearemos la misma ecuación que antes: la clave será medir la probabilidad y el impacto. El ejemplo clarificador de la AEPD es éste:

> *Ante un riesgo de acceso no autorizado por parte de terceros en un proceso de autenticación, el hecho de establecer un usuario y una contraseña asignados al usuario (cumplimiento con políticas de control de acceso e identificación), reduce significativamente la probabilidad de que un tercero pueda realizar un acceso no autorizado. En este caso, la medida de control reduce la probabilidad de ocurrencia del riesgo y, por tanto, minimiza el riesgo residual asociado.*
>
> *Ejemplo práctico de estimación del riesgo residual:*
>
> ***Ciclo de vida del dato** (fase almacenamiento): Almacenamiento de datos de clientes en dispositivos móviles.*
>
> ***Amenaza:** Pérdida del dispositivo móvil.*
>
> ***Riesgo:** Acceso no autorizado por parte de terceros a datos de salud (violación de la confidencialidad).*
>
> ***Impacto:** Violación de derechos fundamentales (Significativo: valor 3).*
>
> ***Probabilidad:** Se puede producir cada vez que el usuario no tiene en su poder el dispositivo móvil (Significativa: valor 3).*
>
> ***Riesgo inherente:** Impacto (3) x Probabilidad (3) = 9 (Riesgo alto).*
>
> ***Medidas de control:** Método de autenticación mediante usuario, contraseña y huella biométrica. Cifrado del dispositivo móvil y pseudonimización de los datos.*
>
> ***Eficacia del control:** Reduce la probabilidad a despreciable (1), debido a que, aunque se pierda el dispositivo, no será posible el acceso sin credenciales. Adicionalmente, reduce el impacto a despreciable (1), debido a que, aunque se pierda el dispositivo, los datos nunca serán identificables evitando producir daños sobre los interesados.*
>
> ***Riesgo residual:** Impacto (1) x Probabilidad (1) = 1 (Riesgo bajo)*

Hablamos de ese riesgo que nos "sobra" una vez calculado el impacto que tienen los controles aplicados. Todas estas proporciones numéricas deberán ser obtenidas de una tabla comparativa de factores. Conviene recordar que en su considerando 75, el RGPD nos ofrece una relación:

Los riesgos para los derechos y libertades de las personas físicas, de gravedad y probabilidad variables, pueden deberse al tratamiento de datos que pudieran provocar daños y perjuicios físicos, materiales o inmateriales, en particular en los casos en los que el tratamiento pueda dar lugar a problemas de discriminación, usurpación de identidad o fraude, pérdidas financieras, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, reversión no autorizada de la seudonimización o cualquier otro perjuicio económico o social significativo; en los casos en los que se prive a los interesados de sus derechos y libertades o se les impida ejercer el control sobre sus datos personales; en los casos en los que los datos personales tratados revelen el origen étnico o racial, las opiniones políticas, la religión o creencias filosóficas, la militancia en sindicatos y el tratamiento de datos genéticos, datos relativos a la salud o datos sobre la vida sexual, o las condenas e infracciones penales o medidas de seguridad conexas; en los casos en los que se evalúen aspectos personales, en particular el análisis o la predicción de aspectos referidos al rendimiento en el trabajo, situación económica, salud, preferencias o intereses personales, fiabilidad o comportamiento, situación o movimientos, con el fin de crear o utilizar perfiles personales; en los casos en los que se traten datos personales de personas vulnerables, en particular niños; o en los casos en los que el tratamiento implique una gran cantidad de datos personales y afecte a un gran número de interesados.

¿Y si al realizar la EIPD nos devuelve un riesgo no aceptable?

Si el nivel de riesgo residual es alto, si a pesar de las medidas de seguridad planificadas el resultado de la ecuación no es satisfactorio, debemos parar el proyecto de tratamiento y buscar garantías suficientes. Es el momento (art. 36.1 RGPD) de que el responsable consulte a la AEPD (a la autoridad de control correspondiente) sobre la viabilidad de esa operación de tratamiento. Es pues el responsable quien, una vez completada la EIPD y esta dar un alto riesgo para los derechos y libertades de las personas tras haber aplicado medidas para mitigarlo, quien consulta a la AEPD. Y cuanto antes mejor, pues sin respuesta no podremos poner en práctica el tratamiento. Una vez la agencia reciba nuestra consulta en ocho semanas nos responderá, aunque si el problema es complejo, el plazo se amplía en seis semanas más. Incluso puede paralizar esos plazos mientras obtiene toda aquella información necesaria.

Para evitar esos retrasos lo mejor es reunir toda aquella información precisa en el primer momento. ¿Qué información? La que se nos indica en el art 36.3 del RGPD.

- Responsabilidades respectivas del responsable, corresponsables y los encargados implicados en el tratamiento, en particular en caso de tratamiento dentro de un grupo empresarial.
- Fines y medios del tratamiento previsto.
- Medidas y garantías establecidas para proteger los derechos y libertades de los interesados.
- Si existe, datos de contacto del DPD.
- Por supuesto, la EIPD completada.
- Cualquier otra información que solicite la autoridad de control.

En el momento en que la AEPD nos responda de forma positiva, habremos concluido la EIPD. Pero… ¿y si la AEPD dice no? Si el informe es desfavorable, no podemos iniciar (y si está en marcha debemos parar) el tratamiento.