
¿Está preparada
tu empresa para cumplir el GDPR?

¿ESTA TU NEGOCIO PREPARADO PARA EL NUEVO RGPD/LOPD?

Las reglas de juego están a punto de cambiar para las empresas que trabajen con datos personales de ciudadanos de la Unión Europea.

El 25 de mayo de 2018 se hace efectivo el nuevo RGPD (Reglamento General de Protección de Datos).

Si tu empresa trabaja con datos personales de ciudadanos de la Unión Europea, a partir del 25 de mayo de 2018 estarás obligado a cumplir con el nuevo ***Reglamento General de Protección de Datos***


vozpopuli > EMPRESAS

LEY DE DATOS

Las pymes españolas incumplen la nueva ley de datos: se exponen a multas de 20 millones

La llamada GDPR obliga a las empresas a modificar su forma de gestionar los datos personales. Las mayoría de las pymes españolas no cumple con los requisitos. A partir del 25 de mayo se aplicarán sanciones

Un ordenador

¿ESTA TU NEGOCIO PREPARADO PARA EL NUEVO RGPD/LOPD?

- **NECESIDAD DE PREPARARSE PARA AFRONTAR EL RGPD.**
- **NOVEDADES Y PLANTEA RETOS IMPORTANTES A LAS EMPRESAS:**
- **SANCIONES MUY ALTAS POR INCUMPLIMIENTO**
- **POSICIÓN ACTIVA DE LA AGENCIA DE PROTECCIÓN DE DATOS**

1.1Calendario

25 de mayo de 2018, empieza a aplicarse el Nuevo Reglamento de Protección de Datos.

Calendario

- RECLAMENTO ENTRÓ EN VIGOR EN MAYO 2016 PARA COMENZAR LA ADAPTACIÓN
- ES APLICABLE DIRECTAMENTE A LOS PAISES MIEMBROS A PARTIR DEL 25 DE MAYO
- ESTÁ EN TRÁMITE DE APROBACIÓN LA FUTURA LOPD QUE DEBE COMPLEMNTAR Y COMPLETAR AL REGLAMENTO

QUEDAN DEROGADAS POR LO TANTO

- La ley orgánica de protección de datos 15/1999.
- Real Decreto 1720/2007 (que nos indicaba las medidas de seguridad que tenía que aplicar una empresa, dependiendo en el nivel en que se encontraba).
- Instrucción 1/2006 sobre sistemas de Video vigilancia.
- Directiva 95/46 del Parlamento Europeo.
- NUEVO desde 25/05/2018
- Reglamento (UE) 2016/679 (RGPD)(Normativa Europea)(normativa de referencia)
- Nueva Ley Orgánica de Protección de Datos (A día de hoy solo conocemos el anteproyecto)(matizara ciertos aspectos que permite el Reglamento)
- Normativa Nacional (Aprobada en Consejo de Ministros en nov-17, pero aún sigue en tramitación para su publicación)

1.2 Normativa

Actual

- LOPD 15/1999
- Real Decreto 1720/2007
- Instrucción 1/2006 Sistemas de Videovigilancia
- Directiva 96/46 del Parlamento Europeo

Futuro

- Reglamento (UE) 2016/679 (RGPD)
- Ley Orgánica de Protección de Datos (A día de hoy se reconoce el anteproyecto)

1.3 Finalidad RPGD

"Proteger los derechos y libertades fundamentales de las personas físicas particular, su derecho a la protección de datos"

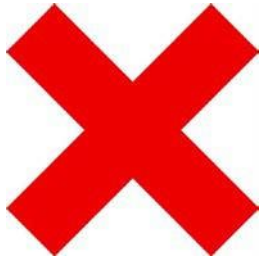
1.4 ¿Quién está obligado?

Todas las empresas que manejemos datos de carácter personal, tanto en soporte informático como en papel.(esto es así desde el 2007, aunque la empresa solo tenga datos en fichero papel, también tiene la obligación de cumplir con la normativa)

¿SI?…….

- Organismos públicos
- Empresas privadas
- Autónomos
- Comunidades de vecinos
- Clubs deportivos
- Asociaciones, etc.

¿NO?



* Particulares

1.4 ¿Qué es un dato de carácter personal?

- Nombres
- DNI
- Direcciones
- Correo electrónico
- Dirección IP
- Datos biométricos
- Etc.

- Todo aquello que bien por separado o bien en conjunto nos hace identificable a una persona

¿Cuándo una empresa no tiene que cumplir con el Reglamento?

Sólo en casos muy particulares, entre los que no se encuentran nuestras empresas, por ejemplo :
Una panadería, que sólo me dedico a vender pan, y no recojo datos de mis clientes, no tengo trabajadores, no mando publicidad, no tengo video vigilancia en mis instalaciones, no tendría que cumplir con el Reglamento, ya que no recojo ni trato ningún dato de carácter personal.

En el momento que tenga alguna de estas cosas, trabajadores, video vigilancia, mande publicidad o tenga un comercio electrónico, ya tendría la obligación de cumplir con la normativa.

Ubicación

Misma normativa de todos los países miembros de la UE.

Empresas ubicadas en la Unión y realicen los tratamientos en la Unión.

Responsable o Encargado que no tengan su sedeen la Unión y oferten bienes o servicios a usuarios de la UE.

Como hemos dicho, la normativa de referencia, a partir del 25 de Mayo, va a ser la normativa europea, ¿esto qué significa?, que todos los países miembros vamos a tener la misma referencia.

A día de hoy, en todos los países miembros hay una Ley de Protección de Datos. En este momento, estas leyes en unos países son muy exigentes, y en otros muy poco exigentes. Pues bien, a partir del 25 de Mayo todos tendremos el mismo reglamento. Esto va a significar que todas las empresas que estemos en la Unión o realicemos tratamiento de datos en la Unión, vamos a tener que cumplir con el Reglamento. También ser indica que aquellos responsables o encargados del tratamiento, es decir, empresas que subcontratemos para prestarnos un servicio, y que ese servicio que presta el encargado o responsable, signifique que vayan a tratar datos de ciudadanos de la Unión, estas empresas también tendrán que cumplir con el nuevo reglamento. Por ejemplo, subcontratamos un servicio de copias de seguridad y es una empresa americana, en el momento en que va a recoger y va a guardar nuestros datos de carácter personal, va a tener la obligación de cumplir con el nuevo reglamento.

2.1 Principio relativos al tratamiento

- Minimización de los datos.
- Exactos y actualizados.
- Limite la finalidad.
- Licitud, lealtad y transparencia don el interesado.
- Limitación del plazo de conservación.
- Integridad y confidencialidad.

¿CÓMO QUEDA EL DERECHO DE INFORMAR, Y CÓMO DEBO PEDIR LOS CONSENTIMIENTOS?

Con el nuevo reglamento lo que se pretende es que las empresas a la hora de recoger datos intenten minimizarlo, es decir, que las empresas no tengamos base de datos con datos que no necesitamos para absolutamente nada. Es decir, si yo te voy a vender un ordenador, y tengo que hacerte una factura, no necesito para nada pedirte la fecha de nacimiento, o datos similares que para hacerte una factura no necesito.

También incide en que los datos que manejemos tienen que ser exactos y actualizados, es decir, que si descubrimos que en nuestra base de datos hay algún dato el cual no está actualizado, lo que debemos hacer es actualizar esa información o bien eliminarla. Que tengamos bien claro el límite de la finalidad para la que están recogiendo los datos de carácter personal. ¿Por qué? Porque a la hora de informar se lo tendremos que decir al usuario o al cliente, que cuando recojamos los datos, lo hagamos siempre de una manera leal, lícita y transparente respecto al ciudadano, que limitemos el plazo de conservación, es decir, la información no tenemos que guardarla de por vida, salvo que haya una ley que nos lo autorice, o que nos obligue más bien a ello, o bien que tengamos la autorización por parte del ciudadano. Es decir, en el caso de facturas de ventas, estaré obligado a guardarlo 6 años, transcurridos los cuales, los tendría que eliminar, que es el tiempo que me marca la obligación legal. También que esos datos que manejemos los tratemos de manera íntegra y confidencial

2.2 ¿Cómo obtener los datos?

Del propio interesado.

Obligación de informar o pedir consentimiento en el momento de la obtención de los datos.

O de un tercero.

Se debe informar al interesado en el plazo máximo de un mes.

En la primera comunicación con el interesado.

Si se comunican a otro destinatario antes de la comunicación.

DEL PROPIO INTERESADO O DE UN TERCERO

Que los obtenemos del interesado, tenemos la obligación de informar y en ciertos casos pedir los consentimientos, y esto se debe producir en el momento que obtengamos la información,

Que los obtenemos de un tercero, tenemos la obligación de informarles, en el plazo máximo de 1 mes o bien en la primera comunicación que tengamos con ese nuevo cliente, usuario o interesado.

Si además los datos se los vamos a comunicar a otro destinatario, también se lo tendremos que comunicar antes de la notificación.

2.3 Base legal para el tratamiento

El tratamiento de los datos debe fundamentarse en:

- Relación contractual.
- Obligación legal para el responsable.
- Intereses vitales del interesado o de otras personas.
- Interés público o ejercicio de poderes públicos.
- Intereses legítimos prevalentes del responsable o de terceros a los que se comunican los datos.
- Consentimientos.

<u>Siempre que recojamos datos tenemos la obligación de informar y de recoger los consentimientos.</u>

Si esos datos se los vamos a comunicar a un tercero, también le tendremos que informar antes de la comunicación.

<u>El tratamiento de los datos debe fundamentarse en:</u>

- **Relación contractual**
- **Obligación legal por la ley fiscal, al tener que hacerte una factura necesito esos datos**
- **Intereses vitales del interesado o de otras personas. En el caso de estar en riesgo tu vida, por ejemplo ante un médico, no se van a pedir esos datos de inicio, sino que se informará después de haber tratado al paciente.**
- **Intereses públicos o ejercicio de poderes públicos, para las Administraciones públicas.**
- **Intereses legítimos prevalentes del responsable o de terceros a los que se comunican los datos**
- **Consentimientos**

Básicamente las empresas nos vamos a centrar en 3 aspectos. Requiero los datos porque hay una relación contractual, o porque tengo una obligación legal, o los consentimientos.
Los consentimientos, por ejemplo los necesitaría una empresa que manejen datos de salud, ya que necesitan nuestro consentimiento para tratar los datos de salud del paciente.
Si por ejemplo se les está mandando publicidad, también se necesita un consentimiento del destinatario.

2.4 ¿Cómo informar?

Nuevos

- Formulario papel.
- Formulario Web.
- Entrevista telefónica.
- Registro aplicaciones móviles.
- Etc.

Antiguos

* Correo postal.
* Correo electrónico.
* Etc.

¿Cómo informar?

Lo que la Agencia aconseja es que se haga a través de los formularios de recogida de datos, ya sea en formulario de papel o a través de la página web, en el cual se pide nombre de usuario, correo electrónico del usuario y consulta, aquí lo normal es aceptar la política de privacidad mediante un check. Mediante esa política de privacidad se informa de todo lo que nos va a obligar el nuevo Reglamento. También si tengo una aplicación móvil en la que el usuario tiene que registrarse, en el momento del registro tengo que informarle.

He de informar del Reglamento a los nuevos clientes a la hora de recoger sus datos, pero también tengo que informar a los "ya clientes". En este caso, si existe una relación contractual o una obligación legal, pero no necesitas consentimiento, lo puedes hacer mediante correo postal, correo electrónico. Si el tratamiento se basa en un consentimiento, y dicho consentimiento a día de hoy no puedes demostrar que lo tienes, tendríamos que mirar a todos esos clientes y obtenerlo. Por ejemplo, si voy a mandar publicidad y no tengo nada que me autorice a su envío, tengo que actualizar y pedir el consentimiento a mis clientes.

2.5 Información

LOPD

- Existencia de fichero, finalidad y destinatario.
- Carácter obligatorio o no de la respuesta.
- ARCO
- Datos del responsable.

¿DE QUÉ TENGO QUE INFORMAR?

A día de hoy con la LOPD ya tenemos la obligación de informar, hasta ahora de lo que se informaba es de que había un fichero, de cómo y para qué tratábamos los datos de ese fichero y de si había destinatarios de cesiones o comunicaciones de datos, además de le carácter obligatorio de dar respuesta, de ofrecerle al usuario sus derechos de acceso, rectificación, cancelación y oposición (derechos ARCO) e identificar al responsable.

Esto hasta día de hoy se hacía en las facturas, pero con la implantación del nuevo Reglamento, no es válido, porque habría que informar ANTES de incorporarlo a nuestra base de datos, no sería correcto informar a través de la factura.

2.5 Información

RGPD

Título	1ª capa	2ª capa
Responsable	Identidad	Datos de contacto Datos de representante DPD
Finalidad	Describir fines	Descripción detallada de fines Plazo de conservación Perfiles
Legitimación	Base Jurídica	Detallar base Obligación o no de dar datos Y consecuencias de no darlos
Destinatarios	Si hay cesiones	A quién o categoría
Derechos	Referencia a los derechos	Cómo ejercerlos Retirar el consentimiento Reclamar ante la AEPD
Procedencia	Fuente	Origen de los datos Datos que se tratan

Con el nuevo reglamento tengo que informar de bastantes más cosas que antes. Se aconseja dividir en epígrafes la información que vamos a presentar al usuario:

- **Responsable**
- **Finalidad**
- **Legitimación**
- **Destinatarios**
- **Derechos**
- **Procedencia, si los datos los he obtenido de un tercero y no directamente del interesado, habrá que informar de dónde proceden esos datos.**

Todo esto lo puedes plantear en dos capas, una primera capa que le presentes al usuario, que sea una cláusula sencilla y muy clara, en el momento de recogida de datos, y una segunda capa en la cual le informes de todo lo que te exige el Reglamento. En la primera capa haces referencia a que la información completa de protección de datos la podrá usted consultar en el dorso de este documento, o a través de una página web que se ponga a disposición del usuario, a través de un correo electrónico es decir que le des siempre la opción de conseguir la información completa.

En la primera capa

Que le tengo que ofrecer al usuario, que sea sencilla y clara, le tengo que decir en primer lugar quien es el Responsable, quien va a tratar tus datos, lo segundo, la finalidad, qué tratamiento le voy a dar a tus datos. La legitimación, en este caso es una relación mercantil, una relación contractual con ese cliente. Las cesiones, solamente habrá cesión de datos a otra empresa si hay una ley que obligue o ampare esa cesión. Por ejemplo a la Agencia tributaria si hay ventas superiores a 3.000€… en cuanto a los derechos, haremos una mención de tu derecho de Acceso, Rectificación Cancelación y Oposición, y siempre haremos una referencia a que los derechos completos estarán en la cláusula completa. Y si los datos no los he obtenido directamente del interesado, tengo que informarle de dónde los he obtenido.

En la segunda capa

Que como hemos dicho podemos ponerla a disposición del usuario en otra parte o en otro documento, en cuanto al responsable, tendremos que identificar, no sólo la empresa que hace el tratamiento de los datos, sino sus datos de contacto, cif, teléfono, dirección, datos del representante, que éste será sustituido por el delegado de protección de datos. (Figura nueva que surge con el nuevo reglamento, que no va a ser obligatoria para todas las empresas, sólo para ciertos sectores, para el resto será una figura voluntaria) En la finalidad, volveremos a repetir para qué voy a tratar tus datos, y además te voy a informar del plazo de conservación de esos datos, ¿la voy a guardar hasta los 6 años que me obliga la ley?, ¿la voy a guardar hasta que el usuario me retire el consentimiento o me diga que lo elimine? Además, si con los datos que le pedimos al usuario vamos a elaborar perfiles, le tienes que informar de ello. Por ejemplo," atendiendo a su perfil de compra, le vamos a hacer un perfil para mandarle un cierto tipo de publicidad". En la legitimidad, hay que informar de La obligación o no de dar los datos, y la consecuencia de no darlos. El consentimiento para recibir publicidad, permanecerá mientras que el usuario no lo retire. En los Destinatarios, tendremos que decir a quien voy a dar tus datos o la categoría de los mismos, o el nombre de empresa a la que vamos a dar tus datos, o al tipo de empresas a los que se los vamos a dar. En cuanto a los Derechos, aparte de decirle los derechos que tiene, le tendremos que decir cómo tiene que pedirlos, a través de una dirección postal de un correo electrónico, de un teléfono de contacto, siempre que sean procedimientos sencillos y gratuitos. También recordarle cómo puede retirarme el consentimiento, y que siempre va a tener la opción de reclamarme frente a la Agencia de Protección de Datos. Y como último punto, el de la procedencia, sólo tendremos que informar de dónde hemos sacada tus datos, y qué datos estoy manejando sobre tu persona.

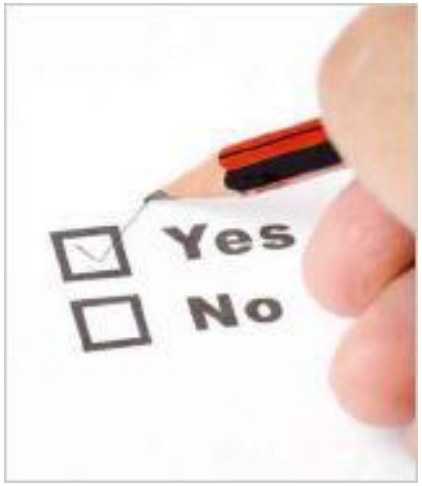
2.6 Consentimiento

El consentimiento debe ser inequívoco (Manifestación del interesado mediante una clara acción afirmativa)

No se admiten consentimientos tácitos o por omisión.

Además debe ser explícito.

- Tratamiento de datos sensibles
- Adopción de decisiones automatizadas.
- Transferencias internacionales.



Si la legitimación de tratar tus datos la basamos en un consentimiento, lo que nos dice el nuevo Reglamento es que esos consentimientos deben ser inequívocos, es decir, que debe de haber una manifestación clara del interesado mediante una clara acción afirmativa, además el consentimiento debe ser explícito si se tratan datos sensibles, si se van a adoptar decisiones automatizadas con la información del usuario, o si se van a realizar transferencias internacionales. Por tanto, siempre vamos a tener que informar si se legitima ese tratamiento en una relación contractual o una obligación legal, y si no siempre vamos a tener que tener ese consentimiento, y éste tiene que ser una acción positiva, hay que marcar una casilla. No se admiten los consentimientos tácitos o por omisión, que hasta ahora sí se permitían. Hay que tener una o dos casillas que tendrá que marcar el usuario. Están terminantemente prohibidas las casillas premarcadas, es el propio usuario el que tiene que marcarlas.

2.7 Derechos

- Acceso.
- Rectificación.
- Supresión (Novedad olvido) DATOS PUBLICADOS.
- Limitación del tratamiento (Novedad).
- Portabilidad (Novedad).
- Oposición. Tratamiento de datos sensibles
- Adopción de decisiones automatizadas.
- Transferencias internacionales.

En la cláusula explicativa vamos a tener que informar de los derechos del usuario a día de hoy se reconocen 4 derechos:

- **<u>Acceso</u> el derecho que tenemos todos a saber que datos maneja una empresa y el tratamiento que le está dando a mis datos.**
- **<u>Rectificación,</u> derecho que tenemos a q nuestros datos sean revisados y rectificados para que estén correctos.**
- **<u>Cancelación</u> (que ahora lo llaman derecho a supresión) derecho que tenemos a que nuestros datos se borren de su base de datos. Va unido al derecho al Olvido, esto es que si mis datos los has publicado en un entorno digital, también tendrás que borrarme de las publicaciones digitales.**
- **<u>Oposición</u> derecho que tenemos para oponernos a que esos datos se utilicen para algo que no sea necesario para el servicio que se nos está prestando, suele hacer referencia a la publicidad.**

Se añaden 2 nuevos derechos:

- **<u>Limitación del tratamiento</u>, esto es el bloqueo de la información, que si la empresa está tratando tus datos, y pones una reclamación para que no los trates, mientras que se resuelve esa reclamación , tendrás que bloquear los datos, y una vez que se resuelva, seguir tratándolos o eliminarlos, según se haya resuelto esa reclamación.**
- **<u>Portabilidad</u> derecho que tenemos a que si vamos a una empresa y pedimos nuestros datos, se nos dé en un formato legible, de forma que yo me vaya a otra empresa y esa empresa los pueda incorporar de forma sencilla a su sistema.**

El plazo de respuesta a cualquiera de estos derechos es de 1 mes. Esta respuesta puede ser de forma positiva o negativa. Por ejemplo me dirijo a una empresa para saber qué datos míos tienen, en principio no deberían tener mis datos… esto lo tendría que pedir por escrito y con acuse de recibo, y en el plazo de 1 mes me tendrían que responder, o bien que no disponen de datos sobre mi persona, o en el caso de que sea positivo, qué datos son los que tienen sobre mi persona.

En algún caso complejo se podría ampliar hasta 2 meses la obligación de responder.

3.0 Encargado de tratamiento

SOLO se podrá contratar encargados que garanticen el cumplimiento del RGPD.

NUEVOS contratos.

- Objeto, duración, naturaleza y finalidad del tratamiento.
- Tipos de datos personales y categorías de interesados.
- Obligación del encargado de tratar los datos personales únicamente siguiendo instrucciones documentales del responsable.
- Condiciones para que el responsable pueda dar autorización previa, especifica o general, a las subcontrataciones,
- Asistencia al responsable siempre que sea posible, en atención al ejercicio de derechos de los interesados. Rectificación.

Los encargados de tratamiento, que ya se reconocen con la normativa actual, son todas las empresas externas que nos prestan un servicio, y que para ello requieren el tratamiento de nuestra información de las bases de datos. El claro ejemplo de encargado de tratamiento sería la gestoría o asesoría laboral con la que trabajamos, que le tenemos que dar los datos de nuestros trabajadores porque nos tiene que hacer las nóminas. Con el nuevo Reglamento, lo que viene a decir es que hay que tener mucho cuidado con la elección del encargado de tratamiento, ya que éste tiene que garantizar que cumple con el nuevo Reglamento General de Protección de Datos (RGPD). ¿Cómo me aseguro de que lo cumplen? A día de hoy con un contrato que nos tienen que firmar, pero en un futuro es muy probable que exista un certificado, un sello de calidad para certificar que la empresa cumple con el RGPD.

Tienes que asegurarte de que te firmen ese contrato garantizando que lo cumplen, y si ya tienes un contrato firmado con ellos anterior, hay que actualizarlo, porque con la entrada en vigor del nuevo RGPD se reconocen nuevas obligaciones para los encargados de tratamiento.

En los nuevos contratos haremos constar :

- **Objeto, la duración, la naturaleza y la finalidad de los tratamientos.**

- **Tipo de datos personales y categorías de interesados (en este caso empleados)**

- **Obligación del encargado de tratar los datos personales únicamente siguiendo las instrucciones documentadas del responsable. Por ejemplo si en este contrato te pongo que tu servicio es el de asesoría laboral, si tú el día de mañana los utilizas para mandar publicidad a mis trabajadores, es tu responsabilidad.**

- **Condiciones para que el responsable pueda dar su autorización previa, específica o general a las subcontrataciones. Imaginamos que esa asesoría que tengo contratada, hay una parte de laboral que no domina y tiene otra asesoría subcontratada para hacer las nóminas, pues bien , esto debe quedar claramente reflejado en el contrato, que el responsable del tratamiento, (nuestra empresa) autoriza a la asesoría a poder subcontratar ciertos servicios necesarios para el cumplimiento del servicio contratado , y que es obligación del Encargado de Tratamiento tener firmado contrato conforme al RGPD con esa subcontratación. De esta forma te vale el contrato firmado por tu encargado de tratamiento, y nos evitaría sanciones por un mal uso del subcontratado o del encargado del tratamiento.**

- **Asistencia por parte del encargado ante posibles reclamaciones de los ciudadanos respecto a sus derechos, en el caso de la gestoría, si un antiguo trabajador te pide su derecho de acceso, la gestoría tiene que decirme que clase de datos maneja para poder decirle al trabajador que información trata nuestra empresa.**

- **En estos contratos también tiene que aparecer que tienes la obligación de cumplir con las medidas de seguridad que establece el RGPD. También que tendrás obligación de comunicar al responsable las brechas de seguridad, porque si hay una brecha de seguridad tenemos la obligación de comunicárselo a la Agencia en el plazo de 72 horas.**

Análisis de riesgos

RESPONSABILIDA PROACTIVA condiciona la adopción de las medidas de seguridad al riesgo que los tratamientos de para los derechos y libertades de los interesados.

El análisis de los riesgos indicara las medidas de seguridad que la organización debe adoptar para garantizar la confidencialidad, la disponibilidad y la integridad de la información y de los sistemas que tratan la misma. Asistencia al responsable siempre que sea posible, en atención al ejercicio de derechos de los interesados. Rectificación.

El análisis de riesgos aparece para cubrir dos aspectos fundamentales que entran con el nuevo reglamento:

- **<u>Responsabilidad proactiva</u>: condiciona la adopción de las medidas de seguridad al riesgo que los tratamientos de datos personales puedan suponer para los derechos y libertades de los interesados.**

- **<u>Enfoque desde el riesgo</u> el análisis de riesgos indicará las medidas de seguridad que la organización debe adoptar para garantizar la confidencialidad, la disponibilidad y la integridad de la información y de los sistemas que tratan la misma.**

En el nuevo RGPD no se indica que medidas de seguridad hay que aplicar, lo que te dicen es que tu empresa tiene que cumplir con las medidas de seguridad que crea oportunas, eso sí , tiene que ser capaz siempre de poder demostrar que la información es confidencial , está disponible, y está íntegra. Quien nos va a determinar qué medidas de seguridad hay que adoptar es el Análisis de Riesgos.

Lo primero que tenemos que identificar es Los Activos, todo aquello que interviene en una protección de datos. Por ejemplo, nuestro servidor donde está la información, es un Activo. Nuestros trabajadores, nuestra copia de seguridad…

El siguiente punto es QUÉ puede atacar a ese activo:

Respecto al servidor, el riesgo puede ser que nos lo roben, que nos entre un virus…

Respecto a los trabajadores, que alguien revele información que no debería…

Además de tener en cuenta los activos y los riesgos que los pueden atacar, y las medidas de seguridad, tenemos una copia de seguridad… hay que tener claro qué probabilidad hay de que se materialice ese riesgo, y se establece un valor. Existen diferentes metodologías para establecer el valor.

Y….

Probabilidad de que se materialice		Impacto	
Ninguna	0	Ninguna	0
Baja	1	Baja	5
Media	2	Media	10
Alta	3	Alta	20

RIESGO = PROBABILIDAD X IMPACTO

NINGUNO	HASTA 00	
RIESGO ACEPTABLE	HASTA 05	ASUMIR RIESGO
RIESGO TOLERABLE	HASTA 10	PROTEGER O MITIGAR EL RIESGO O BIEN COMPARTIR O TRANSFERIR
RIESGO MODERADO	HASTA 20	PREVENIR EL RIESGO, PROTEGER O MITIGAR EL RIESGO O BIEN COMPARTIR O TRANSFERIR
RIESGO IMPORTANTE	HASTA 40	PREVENIR EL RIESGO, PROTEGER O MITIGAR EL RIESGO O BIEN COMPARTIR O TRANSFERIR
RIESGO INACEPTABLE	HASTA 60	EVITAR EL RIESGO, PREVENIR EL RIESGO, PROTEGER O MITIGAR EL RIESGO O BIEN COMPARTIR O TRANSFERIR

5.1 Evaluación de impacto

Tratamientos que supongan un alto riesgo para los derechos y libertades de las personas.

Elaboración de perfiles.

Tratamientos a gran escala de datos sensibles.

Observación sistemática a gran escala de una zona de acceso público.

Esto es una consecuencia del análisis de riesgos. Ya tengo identificados los riesgos, cómo los voy a tratar y cómo voy a actuar en el caso de que ese riesgo se materialice. Esto es una evaluación de impacto. La evaluación de impacto va a ser obligatoria para empresas que traten datos sensibles, datos que supongan un alto riesgo para los derechos y libertades de personas, es decir que realicen perfiles de esas personas, que manejen a gran escala datos sensibles como religión, creencias, salud… o una observación sistemática a gran escala de una zona de acceso público, como video vigilancia a gran escala. Cuando hablamos de " a gran escala", es un término no definido por la Agencia a día de hoy, lo tendrá que aclarar, porque hay quien opina que es a partir de 5.000 clientes, y hay quienes opinan que has de compararte con la empresa más grande de tu sector, y te determinará si manejas volúmenes grandes o no.

5.2 Brechas de seguridad

Comunicar en 72 h. desde su conocimiento ante la AEPD. Encargado de tratamiento deberá notificar las brechas al Responsable.

¿Qué debo notificar?

- Naturaleza y si es posible categoría y nº aproximado de afectados.
- Persona de contacto de la empresa (DPD si existe).
- Consecuencias.

Y…

También se deberá comunicar al interesado, cuando:

- La brecha de seguridad suponga un alto riesgo para los derechos y libertades de las personas físicas.

No será necesario si los datos están cifrados.

A día de hoy, si hay una incidencia, nos roban un servidor, un ordenador o documentación con información, habiendo un riesgo de confidencialidad, de disponibilidad o de integridad de la información tenemos un documento de incidencias que se presenta, y como mucho presentamos una denuncia ante la autoridad. Esto cambia a partir del 25 de Mayo.

Con el nuevo RGPD te dice que si esa brecha de seguridad se materializa, habrá que comunicarlo en un plazo de 72 horas desde que se conozca esa brecha de seguridad a la Agencia Española de Protección de Datos.

Si la brecha de seguridad se produce en nuestro encargado de tratamiento, como es que le hayan robado los datos de nuestros trabajadores a nuestra asesoría laboral, el encargado del tratamiento deberá notificar esa brecha al Responsable para que éste a su vez lo comunique a la Agencia.

Lo que le vamos a decir a la Agencia es la naturaleza, es decir, qué es lo que ha pasado, y si es posible, la categoría, si son datos de clientes, de trabajadores, y el número aproximado de afectados, y de registros afectados, es decir, qué ha pasado y con qué tipo de datos ha pasado. También identificaremos a la persona de contacto de la empresa, para que la Agencia pueda ponerse en contacto con alguien para aclarar lo que ha pasado. Esa persona de contacto, sería el Delegado de protección de datos, en el caso de existir esta figura. A parte de todo esto, hay que explicar las consecuencias de esa brecha de seguridad, qué puede ocurrir, accesos indebidos, mala utilización de la información…
Una vez comunicado a la Agencia, también habrá que comunicárselo al interesado cuando la brecha de seguridad suponga un alto riesgo para los derechos y libertades de las personas físicas. Por ejemplo si te he robado los historiales clínicos. No será necesario comunicárselo al interesado cuando los datos estaban cifrados.

5.3 Delegado de Protección de datos.

¿Para quién es obligatorio?

Organismos públicos, empresas que manejan a gran escala y para determinados sectores.

- Colegios profesionales.
- Sector médico.
- Centros docentes.
- Entidades aseguradoras.
- Publicidad y prospección comercial.

Y ¿Quién puede ser el DPD?

Quien tenga conocimiento e la legislación y la experiencia en la práctica de la Protección de Datos. (Interno o externo)

Se debe hacer público y comunicarlo a la AEPD.

Posición del DPD en las empresas.

Autonomía

Relacionarse con el nivel superior de la dirección.

Que se facilite al DPD todos los recursos necesarios para desarrollar su actividad.

¿Quién puede ser el Delegado de Protección de Datos?

Tiene que ser alguien que conozca la legislación y tenga experiencia en la materia de protección de datos, puede ser un trabajador de la empresa o bien una empresa externa.

Se debe hacer público en tus cláusulas informativas, y comunicarlo a la Agencia. Ya existe una certificación de Delegado, aunque puede ser voluntario y no certificado.

¿Qué posición va a tener mi Delegado?

Tiene que ser una persona que tenga autonomía, que no esté influenciado, y que tenga una vista clara de lo que hay que hacer, que piense por el ciudadano principalmente. Tiene que conocerlo todo de la empresa, se tiene que relacionar con el nivel superior de la dirección, hay que cubrir hasta donde haga falta en materia de protección de datos, y además se le tiene que facilitar todos los recursos necesarios para desarrollar su actividad.

5.4 Registro de actividades

<u>Ya **NO** habrá que inscribir ficheros.</u>

Debe contener:

- Nombre y datos de contacto del responsable o corresponsable y del Delegado de Protección de Datos si existiese.
- Finalidades del tratamiento.
- Descripción de categorías de interesados y categorías de datos personales tratados.

Una de las novedades es que <u>desaparece la inscripción de ficheros</u>.
Lo que sí hay que llevar es un registro de actividades que debe contener:

- **Nombre y datos de contacto del responsable o corresponsable, y la figura del Delegado de protección de datos, si existe.**

- **Finalidades del tratamiento**

- **Descripción de categorías de interesados y categorías de datos personales tratados.**

- **Te dicen que hay que llevar un registro, que va a ser interno, pero que no hay que declarar.**

Este registro de actividades no va a ser obligatorio para todos, sólo va a ser obligatorio para las empresas de más de 250 empleados, y para empresas que traten datos que puedan ser especialmente sensibles, es decir, datos de salud, creencias, religión o datos de condenas de infracciones penales.
Es recomendable que aunque no sea obligatorio, todas las empresas hagan un registro de actividades, ya que va a servir de ayuda para el análisis de riesgos.

Y….

Exentas empresas de <250 empleados, a menos de que el tratamiento que realicen pueda entrañar un riesgo para los derechos y libertades de los interesados, no sea ocasional o incluya categorías especiales de datos o datos relativos a condenas e infracciones penales.

Similar a la estructura de ficheros actual.

5.5 Videovigilancia.

Finalidades.

Preservar la seguridad de las personas bienes, así como de las instalaciones.

Contrato laboral (Informar a los trabajadores)

Novedad

Captación de la vía publica en una extensión superior.Contrato laboral (Informar a los trabajadores)

Garantizar la seguridad de bienes o instalaciones estratégicos o infraestructuras vinculadas al transporte.

Las pautas que nos indica el nuevo RGPD es muy similar, es decir, tengo que tener el cartel a la vista en todos los puntos de acceso al recinto que tenga las cámaras, tengo que tener un documento a disposición del interesado por si nos lo solicita, donde le informo de la videovigilancia.

¿Para qué puedo poner una videovigilancia?

Para preservar la seguridad de las personas y bienes de mi negocio, y para control laboral, siempre informando a los trabajadores.

Por ejemplo, imaginemos que tengo puesta una videovigilancia en mi empresa, no como control laboral, pero sí que en una de las grabaciones aparece un trabajador robando información, dinero o cualquier cosa, la pregunta es si puedo utilizarlo en su contra? El anteproyecto de ley dice que sí, que servirían de prueba, aunque el trabajador podría denunciar por no haberle informado de que la videovigilancia estaba también para control laboral.

Hasta día de hoy las zonas públicas están reservadas para Fuerzas y Cuerpos de Seguridad del Estado, sólo pueden grabar ellos, y las empresas pueden grabar una zona muy limitada, si está grabando la puerta del establecimiento, que grabe la zona de acera más pequeña posible. Como novedad del nuevo RGPD la captación de la vía pública puede ser mayor siempre que sea para garantizar la seguridad de bienes o instalaciones estratégicos de la empresa o para infraestructuras vinculadas al transporte.

5.6 Menores de edad

¿Quién debe autorizar el tratamiento de los datos?

Mayores de 13 años directamente del interesado.(LOPD 14años)

Menores de 13 años autorización de los padres o tutores legales.

La información debe ser concisa, transparenta, inteligible y proporcionado en un lenguaje claro y sencillo

A día de hoy se dice que a partir de los 14 años se pueden obtener directamente de ellos, salvo que haya una ley que obligue a que tengan que estar sus padres o tutores, con el nuevo RGPD, se rebaja la edad a 13 años.
La información debe ser concisas y claras para que las pueda entender el menor.

5.7 Personas fallecidas

Solicitar acceso y en caso su rectificación o supresión.

- Los herederos (Acreditar condición).
- Quien hubiese designado el fallecido.
- Representantes legales o ministerios fiscales.

Hasta ahora no había mención alguna. Con el nuevo RGPD va a haber un derecho de acceso, rectificación y supresión. Ejercido por herederos que acrediten dicha condición, el albacea testamentario o a quien hubiera designado el fallecido en testamento, y en algunos casos los representantes legales o Ministerio Fiscal.

6.0 Sanciones

Se incrementa el importe de las sanciones.

Actualmente rango entre 900,00€ y 600.000,00€

SANCIONES	IMPORTE	PRESCRIPCIÓN
LEVES		AL AÑO
GRAVES	HASTA 10.000.000,00€ O 2% FACTURACIÓN	A LOS DOS AÑOS
MUY GRAVES	HASTA 20.000.000,00€ O 4% FACTURACIÓN	A LOS TRES AÑOS

Y..

TIPO	IMPORTE
LEVES	NO ATENDER LOS DERECHOS NO PUBLICAR LOS DATOS DEL DPD
GRAVES	NO LEGITIMADO NO GARANTIZAR UN NIVEL DE SEGURIDAD ADECUADO CONTRATAR UN ECARGADO QUE NO CUMPLA CON RGPD NO COMUNICAR LAS BRECHAS DE SEGURIDAD
MUY GRAVES	TRATAR DATOS DE UN MENOS SIN SU CONSENTIMIENTO O PATRIA POTESTAD O TUTELA UTILIZACION PARA FINALIDADES INCOMPATIBLES VULNERACION DEL DEBER DE CONFIDENCIALIDAD

¡GRACIAS!

rgpd@legal1.es