REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS (RGPD)

QUÉ ES, A QUIÉN AFECTA, QUÉ NOVEDADES OFRECE...

Introducción

Gestionar una gran cantidad de datos siempre ha sido una tarea ardua y con ciertas dificultades.
Desde la Antigüedad, pasando por el reciente y cada vez más obsoleto uso del papel y, por último, llegando a las actuales nuevas tecnologías con las que podemos tener bibliotecas enteras y bases de datos en la palma de nuestras manos.

Por si eso fuera poco, **tener en nuestro poder ciertos datos sensibles entraña unos riesgos extra**, aunque siempre y cuando se respeten las leyes reguladoras no deberían representar ningún problema.
Dichas normas se han endurecido con el nuevo **Reglamento General de Protección de Datos** Europeo (GDPR, General Data Protection Regulation, **RGPD** según sus siglas en español), aprobado el día 27 de abril de 2016, aunque su **entrada en vigor** no se produjo hasta **el 25 de mayo de 2018.**

El RGPD es el encargado de una regulación capaz de garantizar unas medidas de protección mayores y adecuadas a los nuevos tiempos en cuanto al tratamiento de datos personales de las personas físicas pertenecientes a la Unión Europea.
Hemos confeccionado este documento con el fin de informar a las empresas para que se adapten de la mejor manera al nuevo marco legal.

Os invitamos a efectuar un viaje en forma de lectura que esperamos resulte de gran utilidad.

¿QUÉ SEÑALA EL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS?

El Reglamento General de Protección de Datos (RGPD) **es el nuevo reglamento de la UE relacionado con el procesamiento de datos personales pertenecientes a personas físicas que viven en cualquiera de los Estados miembros de la UE**.

La ley -cuyo nombre oficial es UE 2016/679, de 27 de Abril de 2016- ha derogado a la anterior Directiva 95/46/CE ()LOPD es la que nos regula la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de los mismos en los países pertenecientes a la alianza europea.

Igualmente, **en cada país, se complementará con algunas matizaciones nacionales**.

El RGPD como reglamento unificador

El Reglamento General de Protección de Datos (UE) 2016/679 es un reglamento, más que una directiva, a diferencia de su predecesora, la Directiva de Protección de Datos de 1995 95/46/EC:

- **Una regulación es un acto legislativo vinculante, el cual debe aplicarse en toda la UE.**
- **Una directiva lo que hace es establecer un objetivo que todos los países de la UE deben lograr**, correspondiendo a cada país diseñar sus propias leyes sobre cómo alcanzar dichos fines.

Como consecuencia a la **directiva de Protección de Datos de 1995 95/46/EC, cada estado miembro ha tenido que desarrollar sus propias leyes de protección de datos de forma individual**.

Por ello, las empresas y organizaciones que operan a lo largo y ancho de diferentes países de la alianza europea se encontraron inmersas en todo un gran laberinto legal formado por múltiples leyes.

Afortunadamente, **el RGPD reemplaza esta complejidad con una sola ley unificada que simplifica significativamente la gestión** para las empresas.

¿Es necesario la RGPD? ¿Por qué?

La anterior Directiva 95/46/CE *(LOPD)* fue emitida hace más de veinte años. De mediados de los noventa nos separa ahora mismo todo un océano compuesto por los **enormes cambios tecnológicos, económicos y sociales**, que nos han llevado hasta situación en la que vivimos hoy.

El crecimiento de Internet, las conexiones de banda ancha, los sofisticados dispositivos móviles y las redes sociales, por nombrar solo algunos, han creado una explosión en la forma en que compartimos, almacenamos y procesamos datos personales.

Llevamos nuestros datos en los smartphones, los compartimos en múltiples plataformas y con innumerables entidades, y los almacenamos en ubicaciones como “la nube", de manera intangible e invisible.

Con el crecimiento en el volumen de procesamiento de datos personales, se ha incrementado la **explotación de los mismos para fines fraudulentos,** a pesar del aumento de dinero que, año tras años, se gasta en mecanismos para garantizar la seguridad.

Aquí es donde entra en juego la RGPD, al traer consigo una **legislación reforzada con medidas más estrictas** en la gestión de los datos personales y para implementar normativas adaptadas a los tiempos actuales.

¿A QUIÉN AFECTA EL RGPD Y QUÉ SON “DATOS PERSONALES”?

El reglamento, afecta a **todas aquellas o empresas o compañías que atesoren datos personales de personas físicas de países miembros de la UE. Ello también se aplica a empresas extranjeras, a pesar de que no gocen presencia física en el territorio pero sí posean este tipo de información**.

Respecto al concepto de personas físicas no se debe pasar por alto el detalle de que no se refiere únicamente a los clientes; sino también a ex-clientes, empleados y colaboradores, posibles candidatos a una vacante de los que se haya guardado un CV, usuarios de productos y servicios adquiridos por un tercero, etc.

Dentro del RGPD **es considerado dato personal y, por lo tanto objeto de su regulación, toda aquella información relativa a personas cuya identidad pueda averiguarse, de manera directa o indirecta, a través de alguno de dichos datos**.

> *Por ejemplo, un nombre, la dirección de un domicilio, el número del documento nacional de identidad, etc. También otros datos que hacen referencia a la identidad de la persona en distintos ámbitos –como el físico, psíquico, económico, cultural o social de dicha persona, como fotografías o números de cuenta bancaria- es englobado dentro de la ley (Artículo 4, apartado 1, RGPD).*

Solo hay un tipo de personas físicas sobre cuyos datos no es necesaria la aplicación de la RGPD, las cuales son las personas fallecidas.

1

- Designar un Delegado de Protección de Datos (DPD) **si es obligatorio para la empresa** o si lo asume voluntariamente.
- En caso de no ser necesario designar un DPD, se debe de identificar a la/s persona/s responsables de Coordinar la adaptación.

Consentimiento inequívoco de los interesados

El RGPD requiere que el consentimiento sea "inequívoco", lo que significa que **el interesado deberá de manifestarse mediante una clara acción afirmativa.** Así que, no se consideran formas válidas de obtener el consentimiento el uso **de casillas ya marcadas o la no acción**. En cambio, **sí son acordes al RGPD, la utilización de una declaración por escrito, o la marcación de casillas en un sitio web de internet.**

Además deberán **desagregarse** *(diferentes marcaciónes de casillas / firmas, etc..)* cuando el **consentimiento sea para diferentes fines**, como por ejemplo, tratamiento para la empresa que los recaba de la cesión a terceros.

Consentimiento explícito de los interesados

Existen casos en que además de inequívoco, **el consentimiento ha de ser explícito**:

1. ***Tratamiento de datos sensibles***
2. ***Adopción de decisiones automatizadas***
3. ***Transferencias internacionales***

Los Datos Personales Sensibles son los que pueden entrar en conflicto con los derechos y libertades fundamentales de las personas y han de ser gestionados para dotarles de una mayor protección:

> *la raza del interfecto, su orientación sexual, su orientación política o afiliación sindical, sus creencias religiosas e, incluso, datos biométricos o del ADN que permitan identificar a la persona de manera exacta.*

2

- Elaborar el Registro de Actividades de Tratamiento (servicio de solicitud de copia de la inscripción como ayuda), teniendo en cuenta su finalidad y la base jurídica

En el caso de datos de menores

Dado que los niños merecen una protección específica, cualquier información y comunicación cuyo tratamiento les afecte debe facilitarse en un lenguaje claro y sencillo que sea fácil de entender.

El tratamiento de los datos personales de un niño se considerará lícito cuando **tenga como mínimo 16 años.**

Si el niño es **menor de 16 años, deberá de tener un consentimiento autorizado del titular de la patria potestad** o tutela sobre el niño, y solo en la medida en que se dio o autorizó.

3

Realizar un ANÁLISIS DE RIESGOS:

- Cómo se capturan los datos
- Su Clasificación y Almacenamiento
- Su Uso y/o Tratamiento
- Su Cesión o transferencia a un tercero
- Su Destrucción

El deber de información sobre su recogida es otro de los puntos sensibles. A las obligaciones de informar sobre los ficheros que alojarán la información, la identidad del responsable del tratamiento, la finalidad de la recogida o la puesta en conocimiento de los derechos de acceso, rectificación, cancelación y oposición, **deberá de notificarse el tiempo se conservarán sus datos o a qué autoridades dirigirse en caso de que surja algún problema.**

Por otro lado**, si una entidad obtiene los datos de alguien parte de un tercero** (Artículo 4, apartado 10, RGPD)**, se reduce a un mes el periodo que tiene para informar al interesado de su posesión y procedencia (anteriormente eran tres).**

Así mismo, existe la obligación del responsable del tratamiento de permitir el ejercicio de los mismos de manera telemática. medios aceptados para su eliminación.

Derecho de Supresión "derecho al olvido"

Todo usuario tiene derecho a **limitar la difusión universal e indiscriminada de sus datos personales** en los buscadores generales cuando la información es obsoleta o ya no tiene relevancia ni interés público, aunque la publicación original sea legítima, **suprimiéndola sin dilación indebida** cuando los datos ya no sean necesarios, se retire el consentimiento, se oponga al tratamiento, o que sus datos hayan sido tratados ilícitamente, entre otros.

4

- Revisar las MEDIDAS DE SEGURIDAD una vez se obtengan los resultados del análisis de riesgos

La referencia tecnológica que se engloba en el "derecho al olvido", se refiere a los casos en los que se hayan hecho públicos a través de la Red y cumplan alguno de los puntos anteriores, poniendo la organización los medios necesarios para su eliminación.

El derecho a la transparencia

Este indica que las **informaciones y comunicaciones respecto al tratamiento de datos se ejerzan de una manera explícita y fácil de entender por los interesados, además de ser de fácil acceso**.

> *De esta manera, no ha de quedar ninguna duda de la recogida de datos personales, así como de cuestiones como su fin, el plazo establecido para su tratamiento o quién es el destinatario. También han de ser explicados debidamente los riesgos, normas y derechos que se pueden ejercer respecto a los datos personales, así como las vías mediante las que los interesados pueden hacer valer sus derechos respecto a estos.*

También se ha introducido el llamado **derecho de limitación**, mediante el cual el interesado **puede pedir la limitación del tratamiento de sus datos al responsable de su tratamiento en el contexto de ciertos supuestos**, como la **inexactitud de datos** (permite impugnarlos durante un plazo de tiempo hasta su verificación por parte del responsable); **ilicitud de uso** de datos (si el interesado no quiere suprimirlos, limita su uso)**; para la defensa de reclamaciones o que el interesado se oponga al tratamiento.**

En la práctica, el ejercicio de este derecho se resume en que el responsable del tratamiento podrá conservar los datos pero no utilizarlos.

5

- Establecer mecanismos y procedimiento de NOTIFICACIÓN DE QUIEBRAS DE SEGURIDAD

Derecho a la portabilidad

Tal y como indica la Agencia Española de Protección de Datos, implica que **el interesado podrá solicitar recuperar esos datos en un formato que le permita su traslado a otro responsable**.

Evaluación de impacto (EIPD)

Una medida, que no se contemplaba en la anterior LOPD, y que consiste en que **las organizaciones deben evaluar,** como dice su enunciado, **el impacto en los tratamientos de datos en aquellos casos que puedan implicar un alto riesgo para los derechos y libertades de las personas físicas.**

Dicho estudio debe hacerse antes de iniciar el tratamiento y ha de evaluarse el origen, la naturaleza, la particularidad y la gravedad de dicho riesgo.

La principal meta es reducir los riesgos para la protección de los datos personales y para otros derechos que puedan verse afectados como consecuencia del tratamiento de los datos de carácter personal.

Una EIPD consta, básicamente, de seis fases:

1. Descripción y análisis de la necesidad de la EIPD;
2. Descripción y documentación;
3. Identificación de los riesgos;
4. Evaluación de los riesgos;
5. Gestión y medidas de los riesgos;
6. Revisión e implantación de las medidas.

6

- A partir de los resultados del análisis de riesgos, realizar, en su caso, una EVALUACIÓN DE IMPACTO EN LA PROTECCIÓN DE DATOS

El Encargado de Tratamiento

Su designación **es obligatoria en caso de tratamiento de ficheros de nivel medio/alto** para coordinar la implementación de las medidas de seguridad pertinente.

Este cargo asume competencias en **cuestiones de coordinación y control del cumplimiento de RGPD,** con la obligación de supervisar la aplicación de dichas normas de tratamiento.

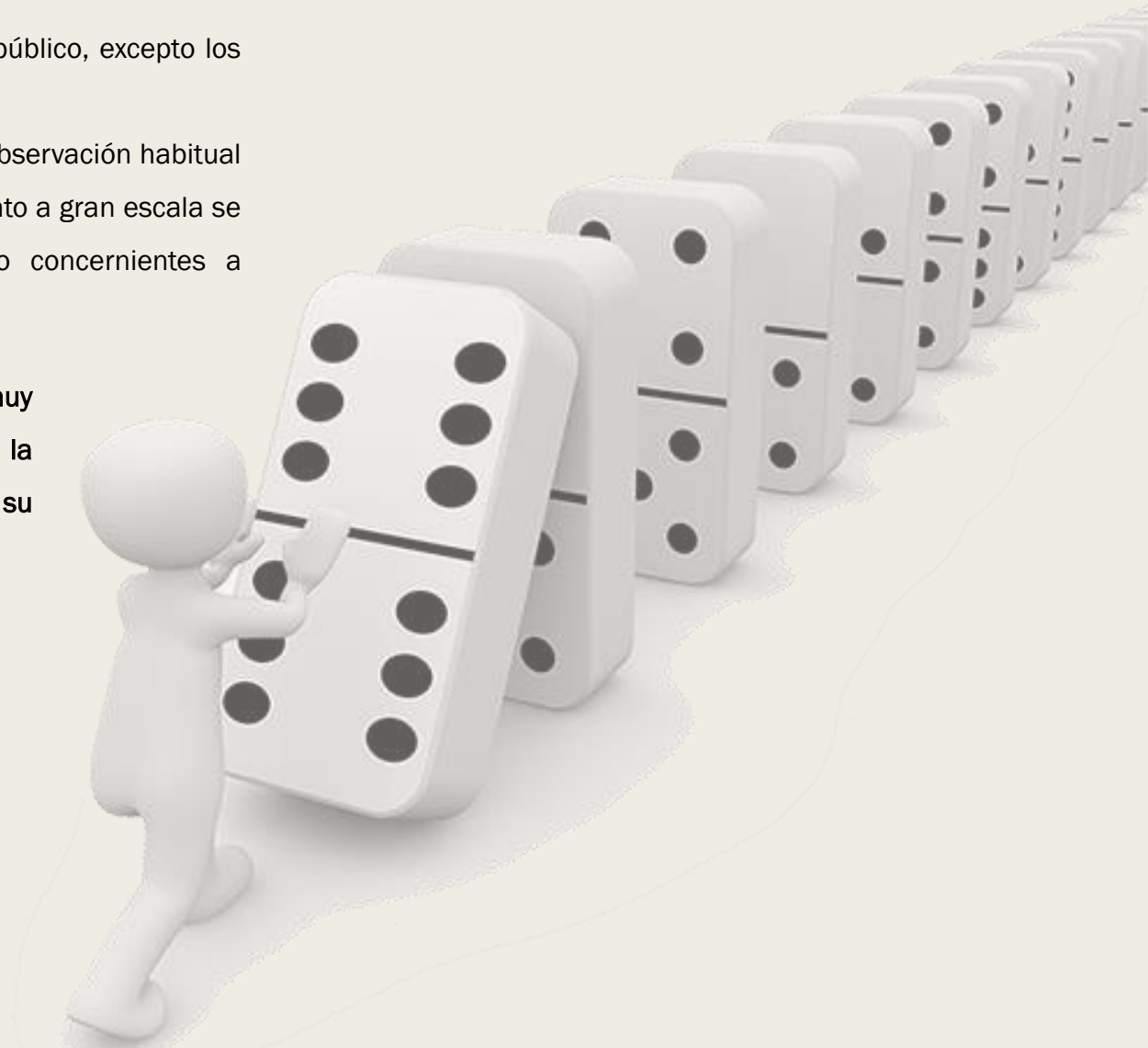
Debe actuar en sinergia con el responsable del tratamiento de datos**, informándole y asesorándole de las obligaciones que debe efectuar para cumplir con el RGPD,** llevando un registro en papel de las comunicaciones entre ambos.

El Encargado de Tratamiento

Así mismo, debe de encargarse de la **documentación, comunicación y notificación respecto a la violación** de datos personales y de **ejercer como enlace con la autoridad de control. Su presencia no será obligatoria siempre** *(con un matiz)* excepto en el caso de tres supuestos:

- Si el tratamiento lo lleva a cabo una autoridad u organismo público, excepto los tribunales que actúen en ejercicio de su función;
- Si las actividades principales del responsable requieran una observación habitual y sistemática de datos a gran escala; y que en dicho tratamiento a gran escala se gestionen datos pertenecientes a categorías especiales o concernientes a cuestiones penales o condenas.

El "matiz" consiste en que **la definición de "gran escala" no queda muy clara** por lo que, aunque en teoría solo es exigible en esos supuestos, **en la práctica se hace necesario en casi todas las empresas debido a su ambigüedad**.



¿Son válidos los contratos anteriores al RGPD?

Los anteriores contratos a la aplicación del RGPD con encargados de tratamiento **deben modificarse y adaptarse** para respetar este contenido.

Utilizar referencias al artículo del RGPD que los regula **no convierte en válido el contrato anterior, aunque se dá un plazo para modificar los contratos pactados de forma indefinida .**

Ya que la Disposición transitoria segunda del Real decreto-ley 5/2018, de 27 de julio, dice que:

> *"Los contratos de encargado del tratamiento suscritos con anterioridad al 25 de mayo de 2018 al amparo de lo dispuesto en el artículo 12 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal* ***mantendrán su vigencia*** *hasta la fecha de vencimiento señalada en los mismos y en caso de haberse pactado de forma indefinida,* ***hasta el 25 de mayo de 2022.***
>
> *Durante dichos plazos cualquiera de las partes podrá exigir a la otra la modificación del contrato a fin de que el mismo resulte conforme a lo dispuesto en el artículo 28 del Reglamento (UE) 2016/679".*

.

FALLOS EN LA SEGURIDAD DE LOS DATOS

La comunicación de fallos de seguridad a la autoridad de protección de datos ha sido convenientemente regulada, ya que **el responsable del tratamiento ha de notificar** a la Agencia Española de Protección de Datos **todos aquellos fallos de seguridad que se produzcan** en su empresa, en un plazo de 72 horas.

Para ello, **ha de disponer de un sistema efectivo para realizar este reporte** a la AEPD o para comunicar el fallo a los afectados si existiera algún riesgo para sus derechos.

Este informe deberá incluir una descripción de la naturaleza del incidente e impacto; el número de interesados afectados y el número de registros; nombre y datos de contacto del delegado de protección de datos; descripción de las posibles consecuencias del incidente; y descripción de las medidas adoptadas o propuestas para solventarlo.

Y para prevenir estos fallos, también están establecidas una serie de medidas en cuanto al registro y la seguridad. De esta forma, **aquellas organizaciones que manejen datos sensibles** o de riesgo para la privacidad de los interesados, **tienen que disponer de un registro** que recoja información de distintas actividades cómo los tratamientos de datos efectuados, su finalidad, datos personales tratados, destinatarios de estos, medidas de seguridad aplicadas… Es decir, todas aquellas actividades realizadas bajo su responsabilidad.

La nueva legislación reseña de "medidas técnicas y organizativas apropiadas" para garantizar un nivel de seguridad adecuado al riesgo.

- *Implementar procedimientos para identificar los incidentes de seguridad, para dar respuesta a los mismos y realizar las necesarias notificaciones.*
- *Evaluar y aplicar la seguridad y realizar regularmente pruebas.*
- *Comprobar la probabilidad de los riesgos cibernéticos.*
- *Asignar la responsabilidad y establecer un presupuesto para el cumplimiento de la protección de datos.*

Sanciones y pérdida de credibilidad

Por último pero no menos importante, no hay que olvidar el régimen sancionador, que se endurece muy notablemente. Las **cantidades que podrían ascender a los 20 millones de euros o el 4% del volumen total de negocio del ejercicio anterior**.

Las empresas que no se adapten pueden enfrentarse, a desembolsos notables con las sanciones. Sin embargo, **no son las únicas consecuencias** del incumpliendo del reglamento.

Las pérdidas económicas también pueden producirse, por ejemplo, por incidentes de seguridad. Éstas quizá conllevarían a una suspensión de los servicios a los clientes, que desamparados, acudirían a la competencia en el mejor de los casos; en el peor, estarían las acciones legales.

También, **se puede provocar un daño en la reputación de la empresa**, que lleve a dicha pérdida de clientes actuales y/o futuros.

Sin embargo, cumpliendo la ley, además de poder evitarse los contratiempos enumerados, **el escenario puede cambiar al otro extremo, ganando clientes, confianza y reputación**.

Por ello se ha de reiterar, una vez más, el cambio legislativo como **una oportunidad de mejora.**

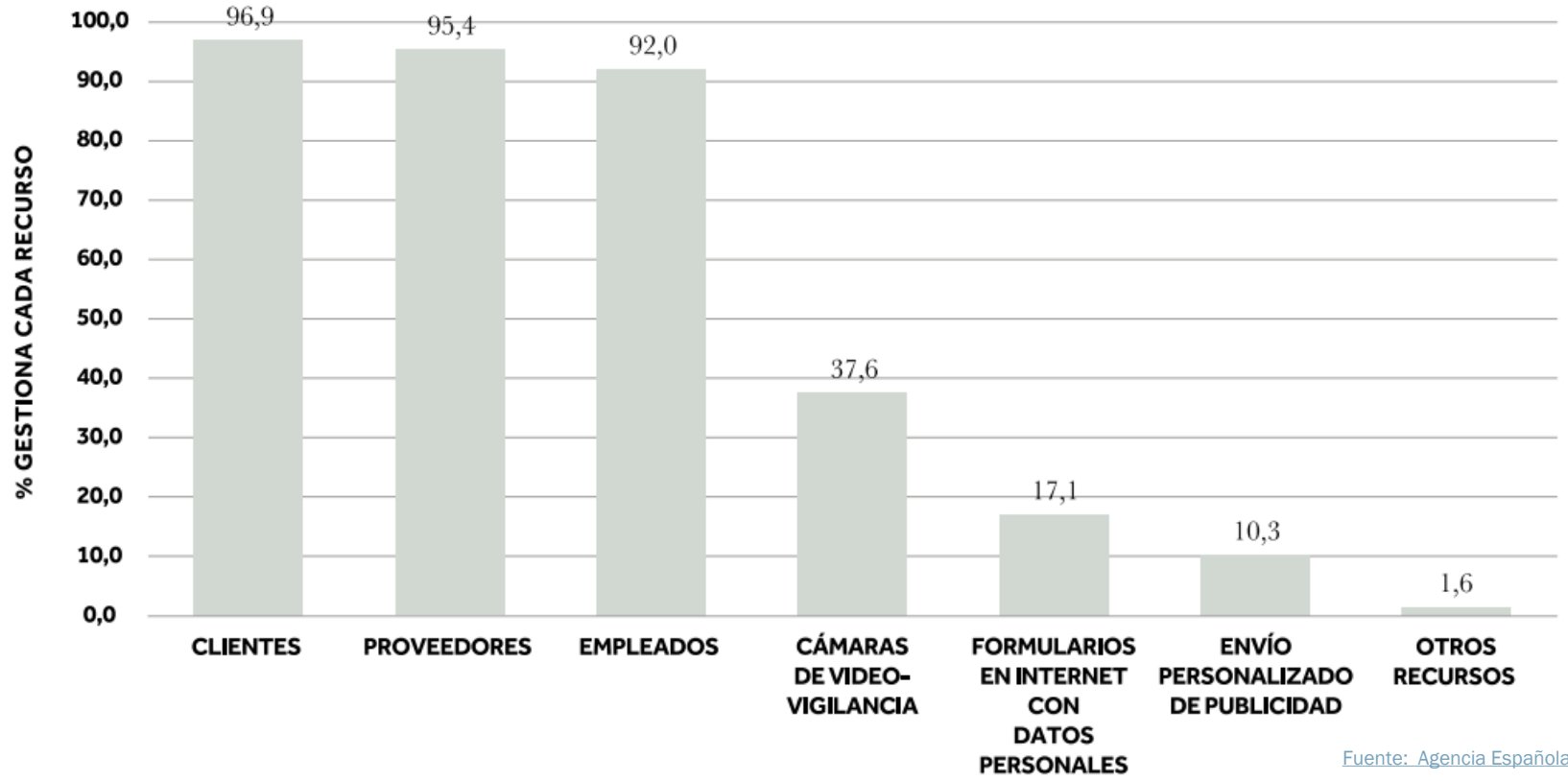
- *Evaluar la posible exposición a responsabilidades con los clientes o proveedores.*
- *Seguimiento de los desarrollos legislativos nacionales que ya que podrían crear nuevas sanciones.*
- Destacar nuestra empresa por un tratamiento impoluto de los datos manejados

ENCUESTA SOBRE EL GRADO DE PREPARACIÓN DE LAS EMPRESAS

La Agencia Española de Protección de Datos, con el apoyo de la Confederación Española de la Pequeña y Mediana Empresa (CEPYME) han hecho una encuesta para obtener información sobre la posición y grado de adaptación de las empresas ante la aplicación de la nueva normativa europea

Recursos Gestionados por las PYMES

Los recursos que gestionan con más frecuencia las empresas de menor dimensión se concentran en tres agregados principales: **los datos de clientes, proveedores y empleados**, que son tratados por prácticamente todas las empresas (del 97% al 92%) y, en menor medida, los recursos relativos a videovigilancia (38%) y formularios en Internet (17%).

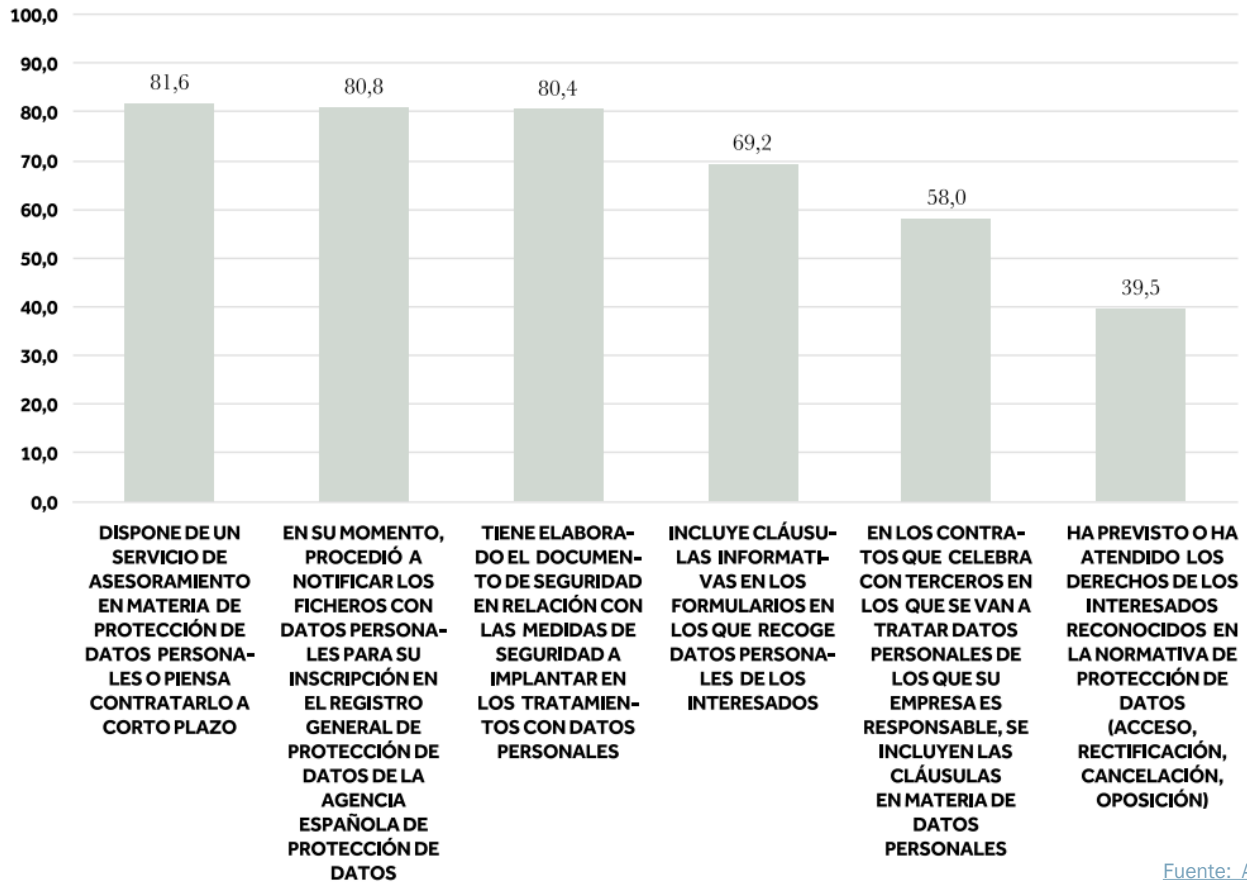


Fuente: Agencia Española de Protección de Datos

Acciones realizadas por las PYMES

En cuanto a acciones concretas, si bien **5 de cada 7 actuaciones cuestionadas han sido ya ejecutadas por la mayoría de las empresas**, éstas tienen un peso desigual:

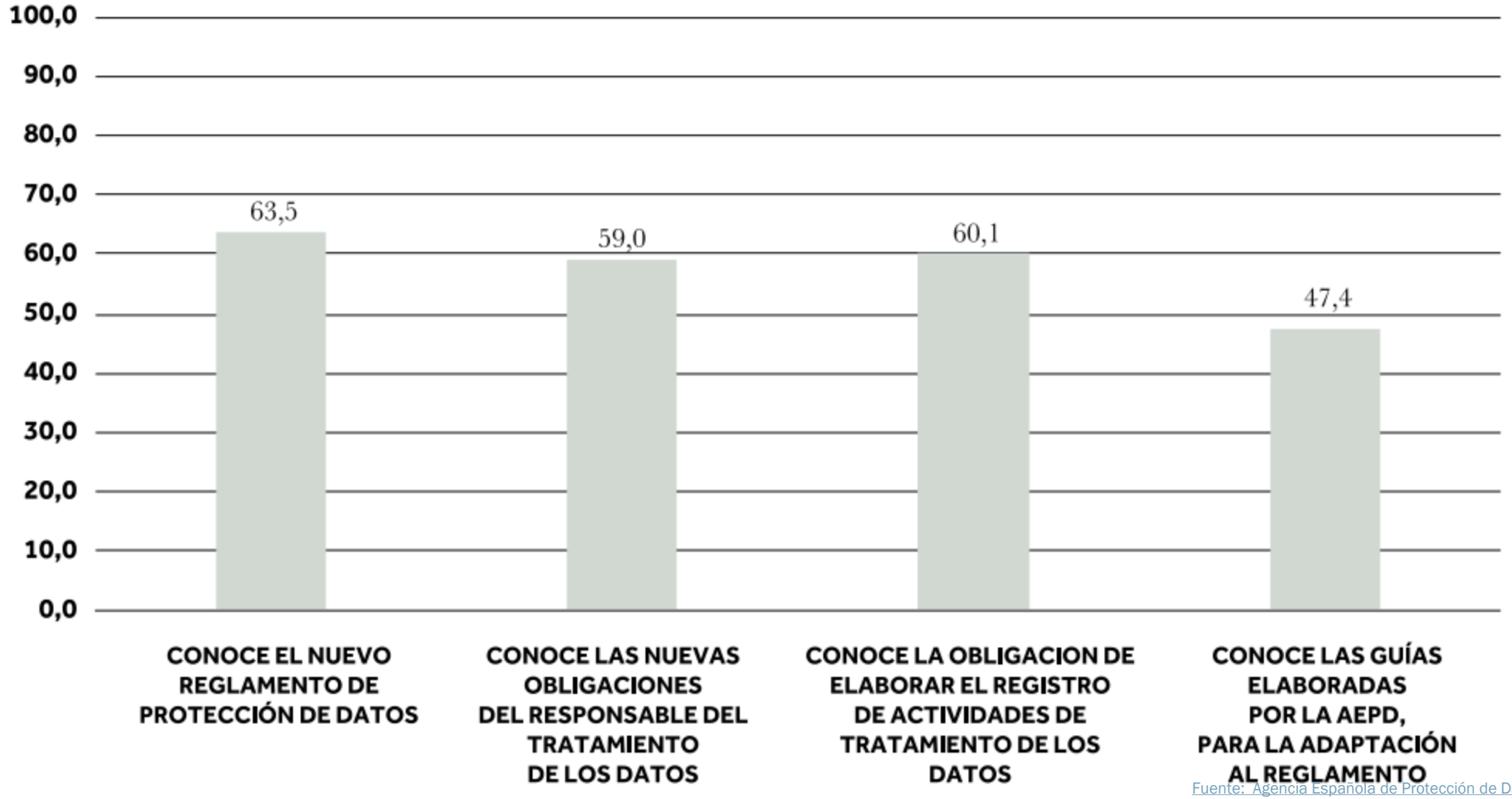
- **Tres de ellas** han sido ejecutadas por más **del 80% de las pymes.**
- **Otras dos** han sido ejecutadas por la mayoría de las empresas, **pero en proporciones inferiores al 70%.**
- Por último, **hay dos actuaciones con una ejecución minoritaria**, que no llega al 40%. Éstas son:
  1.- Ha previsto o atendido solicitudes de ejercicio de los derechos de las personas (39%)
  2.- Uso de la página web de la AEPD (24%)



Fuente: Agencia Española de Protección de Datos

Percepción del conocimiento de la normativa de las PYMES

La extensión del conocimiento de la normativa actual supera en los epígrafes medidos **el 50%, siendo éste algo moderado**



Fuente: Agencia Española de Protección de Datos

Visión de las PYMES sobre la gestión de los datos

Se constata en la encuesta que **son más frecuentes las respuestas positivas** acerca de los mismos por parte de estas entidades.

No obstante, es destacable la distancia que se produce entre la consideración general de la protección de datos y **la consideración de los datos como activo valioso de un negocio, aspecto éste mucho menos detectado por las empresas**, y que, por tanto, no refuerza el impulso de la protección.

	LOS DATOS PERSONALES NO TIENEN VALOR PARA MI NEGOCIO.	LOS DATOS PERSONALES SON NECESARIOS PARA GESTIONAR EL NEGOCIO, PERO LA PROTECCIÓN SUPONE COSTES Y COMPLICACIONES QUE NO COMPENSAN EL VALOR.	LOS DATOS PERSONALES SON LA MEJOR FUENTE DE INFORMACIÓN PARA HACER CRECER Y MEJORAR LAS EMPRESAS.	LOS DATOS PERSONALES DEBEN SER PROTEGIDOS SIEMPRE, ES ALGO QUE NOS AFECTA A TODOS.	AHORA SE DISCUTE MUCHO DE LA PROTECCIÓN Y DEL VALOR DE LOS DATOS PERSONALES, PERO DENTRO DE UN TIEMPO NADIE SE PREOCUPARÁ DE ELLO.
MUY EN DESACUERDO	33,6	22,7	14,8	0,7	19,3
BASTANTE EN DESACUERDO	28,8	23,9	16,6	1,6	24,2
NI DE ACUERDO NI EN DESACUERDO (NO LEER)	10,5	21,0	21,7	6,5	17,5
BASTANTE DE ACUERDO	13,7	20,3	28,5	27,7	23,6
MUY DE ACUERDO	10,9	8,2	15,1	61,9	12,8
N/C	2,6	3,9	3,4	1,6	2,6
RESPUESTAS POSITIVAS	62,4	46,7	43,6	89,6	43,5
RESPUESTAS NEGATIVAS	24,6	28,5	31,3	2,3	36,4

Fuente: Agencia Española de Protección de Datos

LA RGPD ES DE OBLIGADO CUMPLIMIENTO

Más información: aepd.es

GRUPO garatu IT SOLUTIONS

info@grupogaratu.com

grupogaratu.com