

# Kippel<sup>01</sup>

ENTORNO

## Rgpd: enfoque proactivo y sanciones millonarias para blindar al usuario en la Red

“Las compañías tienen el dilema de, por un lado, informar de un modo transparente y obtener los consentimientos individuales pero, por otro lado, saben que haciéndolo así seguramente van a depurar sus bases de datos y van a perder potencial”, explica Joaquín Muñoz, experto de Ontier.

03 ABR 2018 — 05:00

POR D. LÓPEZ / A. PIJUÁN



*Tic tac, tic tac.* Empieza la cuenta atrás para que las compañías de la Unión Europea empiecen a aplicar el nuevo Reglamento General de Protección de Datos (Rgpd) a partir del próximo 25 de mayo. Hasta la fecha, los países de la Unión Europea (UE), las instituciones, las compañías y las organizaciones que tratan con datos han dispuesto de un plazo de dos años para prepararse y adaptarse para la aplicación de esta nueva normativa. ¿Están listos?

**“Creemos que las grandes compañías estarán preparadas para esta fecha, si bien para las pequeñas y medianas empresas (pymes) puede ser más complicado”**, asegura Amalia Pelegrín, directora de *digital policy* de la patronal Ametic, a Kippel01. De un estudio elaborado por la empresa de *software* SAS se desprende que sólo el 56% de las empresas europeas están preparadas para la aplicación del Rgpd.

1/4

<https://www.kippel01.com/entorno/rgpd-enfoque-proactivo-y-sanciones-millonarias-para-blindar-al-usuario-en-la-red.html>

El presente contenido es propiedad exclusiva de Ripley Gestora de Contenidos, SL, sociedad editora de Kippel01.com (www.kippel01.com), que se acoge, para todos sus contenidos, y siempre que no exista indicación expresa de lo contrario, a la licencia Creative Commons Reconocimiento. La información copiada o distribuida deberá indicar, mediante cita explícita y enlace a la URL original, que procede de este sitio.

# Kippel<sup>01</sup>

ENTORNO

**El nuevo reglamento pretende garantizar la privacidad de los ciudadanos de la UE en sus actividades en la Red:** El objetivo es protegerlos del mal uso de los datos por parte de terceros, como puede ser para fines comerciales o políticas fraudulentas. Su aplicación afecta a todas las empresas, independientemente de su tamaño y sector.

**“Muchas pymes creen que no hay que hacer nada hasta el 25 de mayo, pero es todo lo contrario”, explica Joaquín Muñoz (Ontier)**

El derecho a la protección de los datos personales, el incremento sustancial de los flujos transfronterizos de datos o la utilización de estos datos por parte de las empresas privadas y las autoridades públicas son algunos de los motivos que esgrime la UE a la hora de presentar esta nueva normativa, que entró en vigor en mayo de 2016.

“Hay muchas pymes que creen que no hay nada que hacer hasta el 25 de mayo, pero todo lo contrario, ese día habrá que estar en situación de cumplimiento con el reglamento”, apunta Joaquín Muñoz, director del área de IT&IP de Ontier (empresa que trabaja conjuntamente con Exevi en este ámbito).

Según SAS, **menos de la mitad de las compañías es plenamente consciente del impacto que tendrá la normativa.** De su informe *Working Toward RGD Compliance* se desprende que son las grandes corporaciones las que están entendiendo la afectación que tendrá este nuevo marco sobre su negocio, especialmente las del sector de las telecomunicaciones (56%), siendo las empresas públicas las que menos (26%).

**“La aplicación de la norma determina una importante asignación de recursos”, exponen desde Ametic**

Para el experto de Ontier, muchas pymes “todavía están informándose sobre qué es lo que tienen que hacer y sobre las cuestiones que les afecta”. A ello se suma que no se trata de aplicar una serie de condiciones y ya está, puesto que “es una exigencia de cumplimiento continuado”. **“Las empresas deben adaptar sus procesos a las medidas de seguridad exigidas y, además, han de generar evidencias continuadas de su cumplimiento”, indica Muñoz.**

Y es que el Rgpd, que comparte muchos conceptos, principios y mecanismos con la Directiva 95/46 y con las normas nacionales que la aplican, introduce dos grandes novedades: de un lado, el principio de responsabilidad proactiva, de otro, el enfoque de riesgo. **“Uno de los principios fundamentales que distingue a esta normativa del resto es que antes el enfoque era reactivo y ahora es proactivo,** es decir, que la empresa está obligada a demostrar que puede proteger los datos”, señalan desde la Agencia Española de Protección de Datos (Aepd). En cuanto al segundo punto, la nueva normativa estima que la aplicación de sus medidas debe adaptarse a las características de las organizaciones.

2/4

<https://www.kippel01.com/entorno/rgpd-enfoque-proactivo-y-sanciones-millonarias-para-blindar-al-usuario-en-la-red.html>

El presente contenido es propiedad exclusiva de Ripley Gestora de Contenidos, SL, sociedad editora de Kippel01.com (www.kippel01.com), que se acoge, para todos sus contenidos, y siempre que no exista indicación expresa de lo contrario, a la licencia Creative Commons Reconocimiento. La información copiada o distribuida deberá indicar, mediante cita explícita y enlace a la URL original, que procede de este sitio.

# Kippel<sup>01</sup>

## ENTORNO

Si bien aún no existen datos cuantificables de la inversión estimada que han llevado a cabo las empresas estos últimos dos años para adaptarse a la normativa, desde Ametic destacan que “determina una importante asignación de recursos para ello” dado que “implica una exhaustiva revisión de los procedimientos de protección de datos, de análisis y evaluación de los tratamientos realizados y ver si los mismos se adaptan a lo dispuesto en la norma”.



En este sentido, el experto de Ontier pone de relieve que **“una pyme puede dedicar el 80% de sus ingresos a seguridad para que sus datos estén protegidos, pero a lo mejor ese desembolso provoca que su negocio muera”**. Para el experto, la dificultad está en encontrar el equilibrio entre los recursos que se destinan y que estos funcionen.

Pese a ello, tanto la directiva de Ametic como el experto de Ontier coinciden en que la aplicación de esta normativa en España no supondrá un cambio tan radical para las compañías del país. **“Nuestra normativa sobre protección de datos es de las más avanzadas en Europa”**, señala Pelegrín. Muñoz, por su parte, destaca que “se suele mirar a España como un referente, sobre todo por la exigencia que la Agencia Española de Protección de Datos ha tenido durante estos años”.

### ¿Oportunidades perdidas?

El nuevo reglamento proporciona al usuario más control sobre sus datos. Además de los derechos de acceso, rectificación, cancelación y oposición (Arco), el consumidor también tendrá derecho al olvido, derecho a la limitación del tratamiento y derecho a la portabilidad de los datos.

“Si las empresas preguntan de forma individual y transparente a los usuarios para qué quieren que utilicen sus datos, el usuario por defecto va a tender a no dar esa información”, asegura el director del área de IT&IP de Ontier. **“Las compañías tienen el dilema de, por un lado, informar de un**

# Kippel<sup>01</sup>

---

ENTORNO

**modo transparente y obtener los consentimientos individuales** pero, por otro lado, saben que haciéndolo así seguramente van a depurar sus bases de datos y van a perder potencial"; argumenta.

Desde Ametic, en cambio, consideran que ello abrirá las puertas a nuevas oportunidades de negocio. **Pelegrín argumenta que "la adaptación a la norma permitirá el crecimiento del sector**, tanto para implementar la norma como para formar debidamente a quienes deban desarrollar servicios y aplicaciones dirigidas a los usuarios".

## **Sanciones de hasta 20 millones de euros y un 'nueva pieza' en la oficina**

En algunos casos, **infringir el Rgpd puede acarrear multas de hasta el 4% del volumen de facturación anual o sanciones de veinte millones de euros**, lo que suponga el mayor castigo en cada caso. "Ese tipo de sanciones tan altas se reservan para casos flagrantes -señala Muñoz-; lo que se intenta evitar con eso es que las empresas hagan un cálculo para ver si les sale a cuenta incumplir la norma".

Con el fin de asegurar la correcta aplicación de la normativa, **algunas compañías se verán en la obligación de contar con un delegado de protección de datos**. Esta figura será quien se encargue de elaborar un registro de las actividades, realizar un análisis de riesgos, revisar las medidas de seguridad, llevar a cabo una evaluación de impacto en la protección de datos, adecuar los formularios, adaptar los procedimientos para el ejercicio de derechos, valorar si se ofrecen garantías al usuario, así como elaborar o adaptar la política de privacidad a la normativa.

A modo de ejemplo, cualquier ecommerce que trate datos a gran escala tendría que designar un delegado de protección de datos. **"Hay mucho desconocimiento, ha habido años para adaptarse, pero la mayoría no se han puesto", critica el experto de Ontier**, que lamenta que en España, hasta que no empieza a haber noticias en prensa sobre posibles sanciones, la reacción es casi nula.

---

4/4

<https://www.kippel01.com/entorno/rgpd-enfoque-proactivo-y-sanciones-millonarias-para-blindar-al-usuario-en-la-red.html>

---

El presente contenido es propiedad exclusiva de Ripley Gestora de Contenidos, SL, sociedad editora de Kippel01.com (www.kippel01.com), que se acoge, para todos sus contenidos, y siempre que no exista indicación expresa de lo contrario, a la licencia Creative Commons Reconocimiento. La información copiada o distribuida deberá indicar, mediante cita explícita y enlace a la URL original, que procede de este sitio.

---