CONSEJOS ÚTILES PARA EL RGPD*

con Fellowes Brands

¿Cómo me afecta este nuevo reglamento a mí y a mi negocio?

PROTEGE

LOS DATOS DE
MIRADAS CURIOSAS

ARCHIVA

LOS DOCUMENTOS DE
FORMA SEGURA

DESTRUYE

LOS DOCUMENTOS
SIN DEJAR RASTRO

Cordery Legal.Compliance

*Reglamento General de Protección de Datos

¿De qué trata todo esto y cómo están las cosas en este momento?

La Unión Europea (UE) ha cambiado su normativa para la protección de datos. Los cambios han adquirido ahora el rango de ley y se pondrán en marcha en toda la UE el 25 de mayo de 2018. Esta nueva norma recibe el nombre de Protección General de Datos (RGPD, por sus siglas en inglés) y se aplican de forma general, desde a autoridades públicas a pequeñas y medianas empresas. Estos cambios afectarán a la forma en la que todos hacemos negocios. En esta guía se realiza una introducción básica al RGPD y, en particular, se describe el efecto que tiene sobre el trabajo en oficinas.

¿En qué consiste la protección de datos comunitaria?

En la UE, existen normas jurídicas para la recopilación y el procesamiento de datos de carácter personal. Cualquier persona que recopile o procese datos de carácter personal los debe proteger de un uso indebido y cumplir una serie de requisitos jurídicos. El GDPR actualiza las normas existentes en estos momentos.

¿Se aplican estas nuevas normas a los datos electrónicos y a las copias en papel?

Sí. El GDPR se aplicará a los datos electrónicos (como pueden ser mensajes de correo electrónico y bases de datos) y a las copias en papel (con algunas excepciones). Esto significa que también hay responsabilidades con los archivos en papel: tenemos que guardarlos de manera segura y eliminarlos con seguridad (por ejemplo, utilizando una destructora), cuando dejemos de necesitarlos.

Sanciones de hasta

20 millones €

4 % del volumen de negocios anual global de una empresa

¿A qué tipo de sanciones se enfrenta mi empresa en caso de infringir las normas?

Con el nuevo régimen, los reguladores de la protección de los datos pueden imponer unas sanciones altas por la infracción de las nuevas normas. La cota más alta de sanción es un máximo de 20 millones de EUR o el 4 % del volumen de negocios anual global de una empresa, la cantidad que resulte mayor de las dos. Si bien no todas las infracciones desembocarán en la imposición de la sanción más alta, ser sancionado simplemente no es opcional: todos debemos asegurarnos de cumplir las normas.

¿Qué tendrán que hacer más las empresas?

Con las nuevas normas, todas las empresas tendrán más responsabilidades y obligaciones. En concreto, las empresas tienen que llevar a la práctica medidas técnicas y organizativas para asegurarse de estar procesando los datos adecuadamente. Para evaluar el nivel adecuado de seguridad, debe considerar los riesgos que presenta el procesamiento (en particular, derivados de una destrucción accidental o ilícita). También tendrá que poder demostrar las medidas que ha adoptado cuando un regulador le pregunte sobre esas medidas. Una parte importante de ello es comprobar a quién le envía datos de carácter personal. Por ejemplo, también tendrá que comprobar los procesos de las personas con

¿Hay algún ejemplo de casos en los que las personas hayan entendido las cosas incorrectamente?

- **El desconocimiento por incumplimiento puede tener consecuencias.** Hace poco, el regulador de la protección de datos británico, el Information Commissioner's Officer (ICO), sancionó a una autoridad local con 100 000 GBP por no tener en marcha medidas de seguridad para prevenir la pérdida accidental o la destrucción de datos cuando el comprador de un edificio abandonado, que anteriormente había utilizado la corporación municipal, encontró documentos que contenían datos de carácter personal de unas 100 personas (incluidos adultos y niños en circunstancias de vulnerabilidad). Esto se produjo cuando la autoridad local se trasladó de edificio y dejó atrás parte de sus documentos.

- En los Países Bajos, algunos operadores de transporte público fueron sancionados por el regulador de la protección de datos porque guardaban algunos datos de transacciones durante más tiempo que el necesario. En un primer momento, el regulador instó a los operadores a eliminar los datos de las transacciones o anonimizarlos. Los operadores optaron por mantenerlos en el anonimato, pero esto no fue suficiente por lo menos en un caso y, como consecuencia de ello, un operador tuvo que abonar una sanción de 125 000 EUR.

- En España, se han producido varios casos de ejecución por parte del regulador de la protección de datos en los que se había tirado al cubo de la basura o simplemente a la calle documentación que contenía datos de carácter personal. En al menos un caso la documentación solo estaba triturada parcialmente y en otros casos se había tirado a la basura debido a la incapacidad de triturar o eliminar adecuadamente los documentos.

las que trabaja, como pueden ser los servicios de correo, empresas de destrucción y agencias de trabajo temporal.

¿Tendré que reservar un lugar central para la protección de datos en todo lo que hago?

Sí. La confidencialidad se debe incorporar a todos sus procesos. Las empresas tendrán que implantar nuevas formas de garantizar que, por defecto, se procesen únicamente los datos de carácter personal que se necesitan procesar. Como resultado de ello, se tendrá que hacer estas preguntas:

- ¿Necesito estos datos de carácter personal?
- ¿Necesito procesarlos para este fin?
- ¿Todo el mundo que tiene acceso realmente necesita acceder a ellos? (Por ejemplo, si solo RR. HH. debería ver los documentos, ¿deberían estar bajo llave en un archivador y tener solo RR. HH. las llaves?)
- ¿Están desfasados los datos?

¿Será preciso el consentimiento para el procesamiento de los datos?

Sí. En términos generales, debe existir una razón legítima para el procesamiento de datos de carácter personal. Si se necesita el consentimiento para procesar los datos, con las nuevas normas, el consentimiento de una persona se debe haber otorgado de forma libre, específica, informada e inequívoca. El silencio, la exclusión voluntaria o la inactividad no valen y, en su lugar, se tendrá que poner en marcha un proceso activo, como puede ser el de marcar una casilla. Las empresas también tienen que poder demostrar que el consentimiento se ha otorgado de verdad. Asegúrese de tener procesos en marcha que cumplan todos estos requisitos.

¿Se ha introducido algún nuevo derecho?

Sí. Se ha introducido una serie de nuevos derechos, entre los que se incluyen los siguientes:

- El Derecho a ser olvidado: esto permite a las personas pedir la eliminación de sus datos de carácter personal,
- El Derecho a la portabilidad de los datos: esto permite a las personas pedir que sus datos de carácter personal, almacenados en un formato común, se transfieran y,
- El Derecho de oposición: aquí se incluye la posibilidad de las personas a oponerse a que se cree un perfil de ellas. También se pueden oponer al procesamiento de datos de carácter personal para realizar actividades directas de marketing.

La puesta en marcha de estos nuevos derechos, resultará todo un reto para las empresas, si bien debería subrayarse que todos estos nuevos derechos son cualificados, es decir, hay algunas excepciones para las que se deberían asesorar jurídicamente.

¿Qué ocurre si las personas piden ver sus datos?

El derecho de las personas a ver sus datos técnicamente se denomina Solicitudes de acceso a la información pública (SAR, por sus siglas en inglés), sigue existiendo con las nuevas normas. Gracias a este proceso, cualquier persona puede ejercer su derecho a consultar los datos, que se tengan almacenados. Con las nuevas normas, las SAR deben recibir respuesta en el plazo de un mes después de recibirlas (aunque podría haber una ampliación de un máximo de dos meses adicionales en determinadas circunstancias). Además, la posibilidad de que la empresa cobre una tasa para responder a una SAR se ha derogado. Durante los últimos años, se ha producido un aumento significativo del número de SAR realizadas: cuando las SAR resultan gratuitas, es de esperar un aumento mayor del número de ellas. Habida cuenta del aumento de aplicaciones de correo electrónico y en la nube en concreto, ahora las SAR son más costosas y complejas de tratar.

Una parte fundamental de la estrategia futura de protección de datos de cualquier empresa constituirá, por lo tanto, en llevar a la práctica procesos adecuados para tratar las SAR.

Necesitará poner en marcha procesos para lidiar con los **SAR's** *

*Solicitudes de acceso a la información pública

¿Tendré que designar a un encargado de la protección de datos?

Probablemente. Con el GDPR, las autoridades públicas deben designar a un encargado de la protección de datos (DPO, por sus siglas en inglés) y también se tendrá que designar uno para las empresas, cuyo cometido será ocuparse del cumplimiento de la protección de datos en determinadas circunstancias. Una vez más, lo mejor es asesorarse jurídicamente al respecto, en función de lo que se dedique y dónde ejerza su actividad. Habida cuenta de la importancia que el cumplimiento de la confidencialidad tiene hoy en día, incluso si, técnicamente hablando, no se precisa un DPO, hasta una empresa mediana que procese datos de forma habitual debería considerar en cualquier caso la designación de uno.

¿Tendré que informar de infracciones de los datos?

Sí. Garantizar que los datos estén seguros es uno de los pilares de las nuevas normas, entre los que se incluyen abordar las infracciones de datos.

> Qué constituye una infracción de datos abarca muchas situaciones entre las que se incluyen la destrucción, pérdida, modificación, divulgación no autorizada o el acceso a datos de carácter personal.

Se tendrá que informar de las infracciones (incluso qué acción se ha llevado a cabo para paliarlas) al regulador de la protección de datos pertinente, sin un retraso indebido y (cuando sea factible), no más tarde de 72 horas después de haber tenido conocimiento de la infracción. Las personas que se vean afectadas por la infracción también deben ser informadas sin retraso indebido (aunque no se ha fijado ningún límite temporal oficial) cuando dicha infracción es probable que desemboque en un alto riesgo para sus derechos y libertades. Existe un número de excepciones limitadas a la obligación de informar al regulador y a la persona afectada, para las que debería acudir a un profesional para asesorarse debidamente desde el punto de vista jurídico.

Informar sobre las infracciones de datos se complica aún más, debido a lo siguiente:

- El hecho de que algunos países (entre los que se incluyen Austria, Alemania y los Países Bajos) ya cuenten con sus propias obligaciones para informar sobre infracciones de datos
- Informar sobre la infracción de datos puede ser preciso en virtud de otras normas y normativas, en concreto, en los sectores financiero y sanitario
- Hay una legislación independiente adicional que hay que implantar en la UE en línea con lo estipulado en la Directiva comunitaria sobre ciberseguridad

Las empresas deben fijarse como prioridad absoluta la puesta en marcha de un plan de actuación claro en caso de infracción de datos y una política, además de formar al personal

¿Qué ocurre con la responsabilidad y las compensaciones?

Como principio general, cualquiera que haya sufrido un daño como consecuencia de una infracción de las nuevas normas, tiene derecho a percibir una compensación por parte de las personas que controlen o procesen los datos de carácter personal en cuestión por el daño sufrido, con sujeción a determinadas excepciones. Debido al riesgo adicional que puede suponer ahora una vulneración de los datos en virtud de las nuevas normas, especialmente una infracción de los datos, las empresas tendrán que hacer todo lo posible para minimizar el potencial de reclamaciones de compensación.

¿Se tendrá que realizar algún tipo de evaluación del impacto sobre la confidencialidad?

Sí. Con las nuevas normas, estas evaluaciones reciben el nombre de Evaluaciones del impacto en la protección de datos (DPIAs). Cuando es muy probable que las operaciones de procesamiento de datos (en concreto, las que emplean nuevas tecnologías), desemboquen en un alto riesgo para los derechos y libertades de las personas, se debe llevar a cabo una evaluación del impacto sobre la protección de los datos de carácter personal (esto se debe hacer antes del procesamiento). Se debe consultar a un regulador de protección de datos (también antes del procesamiento) cuando una evaluación indique que el procesamiento desembocaría en un alto riesgo si no se adoptan medidas para paliar dicho riesgo.

Es probable que las DPIAs sean algo habitual y deberían confirmarse como una herramienta muy útil para que las empresas atajen los riesgos de confidencialidad, incluidas la evaluación del riesgo de seguridad de los datos y la consideración de los riesgos que presenta el procesamiento de datos de carácter personal, como puede ser la destrucción accidental o ilícita.

¿Ha habido algún cambio con las transferencias de datos a terceros países?

En realidad, no. Las normas especiales que existen en relación a la transferencia de datos de los Estados miembros comunitarios a terceros países (incluido EE. UU.) siguen vigentes con el GDPR, incluido el requisito de que dichas transferencias de datos solo pueden tener lugar cuando esos terceros países garanticen la existencia de un nivel de protección adecuado. Con el nuevo régimen, estas normas ahora están más detalladas. Este es un tema complicado que también hay que desarrollar en virtud de las normas de protección de datos existentes y del que debería hablar con su equipo jurídico.

¿Dónde puedo encontrar más información?

Las nuevas normas están disponibles en el sitio web de la Comisión Europea

¿Qué debo hacer ahora?

Para que tu negocio cumpla el GDPR, debes presupuestar y planificar los recursos (incluidos los informáticos). Utiliza también correctamente tu tiempo de planificación para adaptarse. A continuación, se incluyen las diez normas de cumplimiento más importantes que debería empezar a tratar:

1. Pon en marcha un proceso de evaluación del impacto sobre la confidencialidad, traza un mapa de los datos y fija las zonas de riesgo
2. Revisa en profundidad los contratos de los proveedores, necesitarás que los proveedores te ayuden, sobre todo a la hora de informar de infracciones de seguridad con rapidez, así que asegúrate de tener los derechos contractuales para insistir en este aspecto
3. Actualiza los sistemas, los materiales, elabora nueva documentación detallada y ten listos los registros para la producción en caso de que se produzca una inspección normativa
4. Revisa aspectos prácticos clave, incluida la conservación de datos, con todos los datos que utiliza la empresa
5. Asegúrate de contar con procedimientos para destruir de forma segura los datos que no necesitas
6. Asegúrate de que nuevos aspectos, tales como el consentimiento explícito, el derecho a ser olvidado, el derecho a la portabilidad de los datos y el derecho de oposición, se incluyan en las políticas y en los procedimientos
7. Pon en marcha un procedimiento de notificación de infracciones de datos, que incluya capacidades de detección y respuesta y compruébelo igual que con un simulacro de incendio
8. Considera la posibilidad de designar a un encargado de la protección de datos
9. Formación, formación y más formación: forma al personal en todos los aspectos anteriores (los reguladores de la protección de datos prestan especial atención a esto)
10. Establece y lleva a cabo auditorías de cumplimiento regulares para identificar y subsanar cualquier problema.

Autores:

Jonathan Armstrong y **André Bywater** de **Cordery Compliance** tienen una amplia experiencia en el asesoramiento sobre cuestiones del GDPR y nos han ayudado en la elaboración de este libro blanco.
www.corderycompliance.com

Jonathan Armstrong
Cordery
Lexis House
30 Farringdon Street,
London, EC4A 4HH
+44 (0)207 075 1784
jonathan.armstrong@corderycompliance.com

André Bywater
Cordery
Lexis House
30 Farringdon Street
London, EC4A 4HH
+44 (0)207 075 1785
andre.bywater@corderycompliance.com

Acerca de Fellowes:

Fellowes es fabricante y distribuidor de equipos de oficina, soluciones de archivo y accesorios ergonómicos tanto para el hogar como para la oficina. Todos nuestros productos están diseñados y desarrollados para mejorar la calidad, la eficiencia y la productividad en el trabajo.
www.fellowes.com /es

Fellowes Ibérica S.L.
Pº de las Flores 23, Nave 3
y 4
28823 Coslada - Madrid
91 748 05 01

Cordery® Legal.Compliance

Fellowes Brands™