Restauracióncolectiva
El portal de referencia para los profesionales del sector

Protección de datos: ¿qué supone estar al día con el nuevo reglamento europeo?

Martes, 29 de mayo 2018

A nadie se le escapa que en las últimas semanas algo se mueve en relación a la protección de datos; pero más allá de la 'locura de envíos de e.mails' que se ha desatado, ¿qué supone realmente estar al día con la nueva normativa?, ¿a qué estamos obligados autónomos, empresas y entidades en general?, ¿qué obligaciones específicas tiene una empresa de colectividades por el hecho de manejar datos de salud respecto, por ejemplo, a alergias e intolerancias?

El pasado 25 de mayo entró en vigor la aplicación del nuevo Reglamento General de Protección de Datos (679/2016), reglamento que deroga la actual Ley de Protección de Datos (LOPD). La nueva normativa es la misma para toda Europa y por tanto, todas las empresas y entidades estarán bajo la tutela de la misma norma; con ello la protección de datos será más uniforme y los derechos fundamentales de las personas estarán igualmente protegidos en todo el territorio europeo.

¿Quién está obligado a cumplir con la normativa?

Cualquier autónomo, empresa o entidad que trate datos de carácter personal como por ejemplo nombres, apellidos, direcciones, teléfonos, fotografias… o que trate datos de salud de clientes, trabajadores o colaboradores, está obligado a cumplir con la normativa.

Por todo ello, actualmente es muy complicado encontrar algun empresa que no esté sujeta a la Ley de Protección de Datos ya que habitualmente se tienen, como mínimo, datos de los clientes y trabajadores. También están obligadas por ley, las empresas que tienen cámaras de videovigilancia.

La página web también se debe adecuar a la Ley de Protección de Datos y si se hace venta *online* es necesario adaptarse a unas buenas condiciones de venta y de uso.

La empresa está obligada y es la responsable de los datos y, por tanto, debe adoptar las medidas técnicas y organizativas de seguridad necesarias para garantizar la integridad, disponibilidad y confidencialidad de dichos datos.

¿Qué debemos hacer?

Aunque cada caso es diferente, a nivel general podemos decir que los puntos mínimos para adaptarse a la nueva normativa son los siguientes:

1. Adaptación de las **cláusulas informativas** sobre el tratamiento de datos a la nueva normativa.
2. Obtención del **consentimiento** por escrito de todas aquellas personas de las cuales tratamos datos.
3. Elaboración del **documento de registro de actividades de tratamiento** donde se reflejen la medidas de seguridad, tanto técnicas como organizativas, y los flujos de tratamiento de datos.
4. **Regularización de contratos con terceros** que accedan o traten nuestros datos (gestoría, empresa de soporte informático, empresas de limpieza…) para que nos den la garantía y certifiquen que cumplen con la normativa; debemos tener la certeza de que la empresa cumple con la normativa ya que sino podemos ser responsables de ceder datos a una persona jurídica que no cumple con la protección de datos.
5. Se debe **informar a los afectados sobre la finalidad del uso de sus datos y de sus derechos** de acceso, rectificación, oposición y cancelación, supresión y portabilidad.
6. En el caso de que la empresa disponga de **página web**, se debe elaborar una política de privacidad, aviso legal, cláusulas… en todos los formularios de solicitud de información, altas a boletines informativos, etc.
7. Debemos tener también el **consentimiento expreso** de los clientes, personas y entidades para poder colgar información o imágenes en redes sociales (si no hay consentimiento, no se puede hacer).

Toda esta documentación es de carácter obligatorio sin excepciones. En el caso de requerimiento o inspección de la Agencia Española de Protección de Datos se deberá entregar toda la documentación debidamente confeccionada.

Sanciones que no distinguen entre 'grandes' y 'pequeños'

A diferencia de lo que se venía haciendo hasta ahora, desaparecen las auditorías bianuales y ahora se habla de la responsabilidad proactiva. Las empresas deben cumplir con la ley de manera continuada y actualizada, y deben ser capaces de probar, en cualquier momento, este cumplimiento ante la autoridad competente.

Es importante regularizar el tema y adaptarse a la nueva norma, no solo porque la ley así lo exige, sino porque el incumplimiento comporta un grave riesgo ya que las 'desmedidas' sanciones no distinguen entre grandes y pequeñas empresas (las multas pueden llegar a los 20 millones de euros o el 4% de la facturación anual).

Actualmente se da un elevado grado de incumplimiento motivado por diferentes razones; la principal de ellas el desconocimiento y la falta de compresión de la ley… de forma muy generalizada se piensa que se hace un uso correcto de los datos cuando no es así.

El hecho de estar al día y cumplir con la normativa depura y delega responsabilidades en todos los usuarios que manipulan datos (trabajadores, colaboradores, asesoría, informáticos…). Además, a nivel organizativo la regularización ayuda a optimizar los recursos y, por tanto, mejora la eficacia del sistema de trabajo.

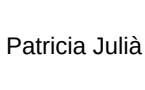
'Delegado de protección de datos' para información sensible como los datos de salud

El nuevo reglamento contempla la figura del 'Delegado de protección de datos' para aquellas empresas que manejan un volumen muy elevado de datos y para las que trabajan con datos sensibles como los referidos a la salud. Es el caso de los servcios de colectividades que, entre otros, manejan datos sobre alergias, intolerancias y otras patologías de sus usuarios.

En este caso se deberá contar con una persona encargada de controlar el tratamiento de datos que hace la empresa y que será quien velará por la seguridad y buen uso de los mismos.

Por último comentar que los cambios también afectan al nivel tecnológico ya que es importante saber quien accede a los datos y qué medidas de seguridad son necesarias para que este acceso sea restringido y seguro. Es necesario verificar también que los servidores donde se guarda toda la información están dentro de la UE.

Cualquier autónomo, empresas o entidad del tipo que sea debe implementar todas estas medidas desde el momento en que empiece a trabajar con datos de terceros.


Patricia Julià

Patrícia Julià es abogada y máster en Derecho de la Sociedad de la información. Trabaja en Seinprodat, una empresa especializada en consultoría jurídica e informática de protección de datos y es delegada de Protección de Datos, certificada por el Ilustre Colegio de la Abogacía de Barcelona. Linkedin.