La privacidad de los datos en la empresa

Author : gochoadealda

Categories : Auditoría, Certificación y Calidad de Sistemas Informáticos

Date : 1 diciembre, 2018

El 25 de mayo de este año, 2018, se terminó el plazo de adaptación que se había dado para que las empresas y entidades de la EU se adaptasen a la nueva ley de protección de datos, la RGPD. A partir de este día el cumplimiento de la RGPD empezó a ser obligatorio, pudiendo ser sancionadas aquellas personas u organizaciones que no cumplan con sus normativas. Por lo tanto, la pregunta es simple, ¿Cuáles son los principales cambios que se deben implantar en las
empresas para cumplir con la RGPD? Pues bien, a lo largo de este post hablaremos de los principales cambios que ha traído consigo la RGPD, como afecta a las empresas y que sanciones puede traer el incumplimiento de estas normativas.
Lo primero que debemos saber es quienes están obligados a cumplir con la RGPD, pues bien, tal y como establece la ley, la RGPD es de obligado cumplimiento para todas las entidades europeas, autónomos y administraciones públicas. Pero además también están sujetos a esta ley todas las personas y entidades que presten sus servicios desde fuera de la UE a usuarios de
la UE o que reciban datos desde la UE, para prestar un servicio fuera.
La RGPD, está basada en el principio de responsabilidad proactiva. Esto significa que además de exigir un debido cumplimiento de todas sus cláusulas es necesario poder demostrar que se cumplen estas cláusulas. Esto implica que las personas y entidades que responden ante la RGPD están obligados a aplicar las medidas necesarias para garantizar la seguridad y privacidad de los datos (cumplir con la RGPD) y además poder demostrar que estas medidas se
están aplicando, funcionan correctamente y son efectivas.
Otro concepto especialmente relevante que trae la RGPD es el enfoque de riesgo. El enfoque de riesgo no es otra cosa que tener en cuenta que las medidas que se apliquen por parte de las
empresas. Para garantizar la seguridad de los datos, deben tener en cuenta la naturaleza, el ámbito del contexto y los fines de tratamiento, así como el riesgo y los derechos y libertades de las personas. En resumen, que datos se manejan, para qué, cómo se tratan y recogen estos datos y el riesgo que implica trabajar con esta información.
La RGPD además de tratar de unificar todas las políticas de protección de datos en una para toda la UE, como comentábamos en el post anterior, trata de instaurar una filosofía de buenas prácticas y protección de los datos de los usuarios, entendiendo siempre a los usuarios como la parte más débil en todos los procesos, centrándose por tanto siempre en su protección. Por ello la RGPD establece que también la concepción, por parte de una empresa o sujeto, de un servicio ya debe tenerse en cuenta la RGPD, por tanto, la privacidad de las personas debe estar
garantizada.

Esto nos lleva a dos principios que se integran en la ley:

- **Principio de minimización:** Los datos personales que se recojan deben de ser los mínimos necesarios para prestar el servicio. Además, los datos requeridos deben de estar en consonancia con el servicio que se presta, tener coherencia.
- **Principio de No compartición:** No se podrán compartir datos de usuarios o clientes a terceros a menos que se reciba un consentimiento expreso de los mismos. En este punto es necesario destacar que la respuesta que se reciba del usuario de cara a su consentimiento debe de ser positiva y que garantice que el usuario comprende perfectamente lo que está aceptando.

Es también obligatorio llevar un registro de todo tratamiento que se haga con los datos. Además, cuando se manejen datos que se cataloguen como alto riesgo, se deberán recoger cuales son estos riesgos y además prever medidas que minimicen el impacto de los mismos. Este análisis de riegos no es de obligado cumplimiento para todas las empresas, solo están obligadas aquellas empresas que manejen datos sensibles de una cantidad relevante de personas o aquellas que trabajen con especialmente sensible de una o más personas. Es también obligado para estos casos en los que se requiera el análisis de riesgos, contar con un Delegado de Protección de Datos o DPD que puede ser interno de la propia empresa o subcontratado de terceros. De este delegado se debe conocer el nombre y los apellidos.
En caso de que pase lo peor, por ejemplo, una brecha de seguridad la RGPD obliga a las empresas a notificar de la intrusión con un plazo máximo de 72 horas. Está notificación deberá ser dirigida a la Agencia Española de Protección de Datos, en el caso de nuestro país, al organismo pertinente en el caso de que la empresa pertenezca a otro país de la UE o sea de fuera de la UE. En el caso de que los datos perdidos o comprometidos sean sensibles es necesario, además de notificar al organismo pertinente, a las personas afectadas por dicha brecha de seguridad.
La RGPD no obliga, pero si invita a las empresas a certificarse, de cara a demostrar que se cumplen con las normativas de la misma. Por otro lado, la certificación es una forma de mostrar una intención activa de cumplir con la protección de los datos y la privacidad de los usuarios.
Al contratar a una empresa o entidad, se debe llevar un registro de actividades. A esto se le conoce como el deber de información, esto es, revisar el clausulado que se emplea en todas las comunicaciones: correos electrónicos, cartas, albaranes, facturas y fichas de clientes entre otras.
Por último, debemos conocer las sanciones a las que empresas y todas las entidades o sujetos pueden enfrentarse en caso de infracción. Con respecto a la LOPD han crecido enormemente. Las sanciones vigentes en la RGPD pueden alcanzar en su máximo, en la categoría de leve, los
10.000.000€ o un 2% del volumen global de negocio y en infracciones graves hasta 20.000.000€ o un 4% del volumen global de negocio. Mientras que en la LOPD eran de 40.000€
y 600.000€ en infracciones leves y graves o muy graves, respectivamente.

Referencias

https://letslaw.es/diferencia-rgpd-lopd/
https://www.sage.com/es-es/blog/nuevo-viejo-lopd-vs-rgpd-infografia/
https://www.pymelegal.es/es/noticias/109/transicion-en-la-proteccion-de-datos---de-la-lopd-al-rgpd.html
https://www.advantic.es/perfiles/rgpd/
https://www.youtube.com/watch?v=XP6117Il_eo