Los principios básicos del procesamiento de datos en los negocios

En los últimos 40 años la tecnología ha cambiado radicalmente la manera que teníamos de hacer negocios.

En 1990 los ordenadores personales eran lentos, pesados e increíblemente caros, y la"*WorldWideWeb*" se encontraba aún en pañales. En la actualidad, 2.500 millones de personas en todo el mundo tienen un smartphone en su bolsillo, en el bolso o en la mano. Un ordenador conectado permanentemente que nos acompaña a todos los sitios.

Nos basamos en los motores de búsqueda para hacer cualquier pregunta, obtenemos las direcciones del GPS, nos comunicamos con nuestras marcas favoritas en las redes sociales y hacemos todas nuestras compras en línea.

Y cómo no, todas estas interacciones implican un intercambio de información. Google sabe lo que buscamos, desde dónde lo buscamos, en qué hacemos clic y cómo interactuamos con una página. Ya ni hablemos de Facebook. **Nuestras aplicaciones de GPS rastrean nuestra ubicación cada vez que nuestro teléfono se enciende**. **Nuestras cuentas de redes sociales están vinculadas a nuestro número de teléfono** y la información de nuestra tarjeta de crédito se guarda la mayoría de las veces junto con nuestra dirección postal.
Entonces, tiene sentido que, a medida que más y más información pasa a estar en la nube, **las empresas tengan un estándar más alto para protegerla.**

El procesamiento de los datos y la importancia de la protección de la privacidad

La gente valora su privacidad. O al menos parece que algo más de lo que lo hacía hace unos años.
Hemos tenido que pasar múltiples *Cambridge Analyticas* para que así sea.
De hecho, **está considerada un derecho humano básico**. Pero dije no hace mucho, la forma en que miramos la privacidad está evolucionando junto con la tecnología. La privacidad ya no se logra simplemente cerrando las persianas o la puerta de nuestra casa. Cosas que antes consideraríamos vulnerar nuestra privacidad *(como exponer nuestro día a día en una página online)* se han vuelto hasta normales en redes sociales.

Que en cada vez más derroteros cuando hablamos de protección de la privacidad, nos referimos a la protección y a la seguridad de los datos. De ese intangible que rige los negocios de nuestros días.
Sin una protección de datos estricta por parte de una empresa, los clientes están en riesgo. A la mente me viene el caso de British Airways *(ES)*. Durante dos semanas en agosto y septiembre de 2018 un fallo de seguridad llevó al robo de la información personal y financiera de aproximadamente 380.000 clientes.

Y es que, mal que nos pese, no solo el robo o el fraude de identidad son las consecuencias de un procesamiento deficiente de los datos.
El procesamiento incorrecto de los datos puede hacer que alguien pase por alto una oportunidad de trabajo, que se pueda manipular información sobre una persona, o se puedan vender datos para realizar publicidad dirigida.

Eso significa que no solo las grandes empresas como Facebook, Google y Amazon deben adherirse a los principios básicos del procesamiento de datos. Las pequeñas empresas, e incluso los autónomos, también debemos procesar los datos de manera justa, transparente y segura.

¿Cuáles son tus obligaciones como empresa?

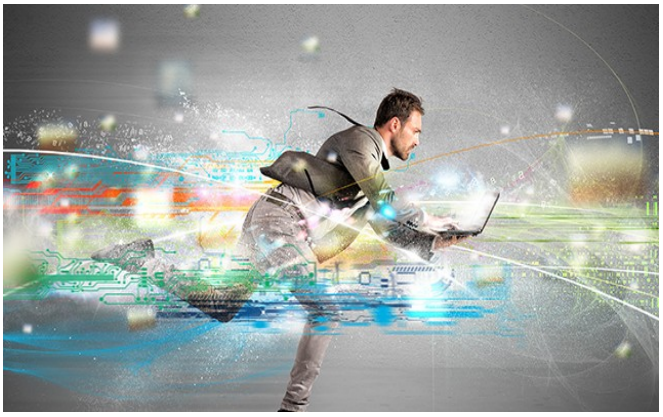
Según la nueva regulación del Reglamento General de Protección de Datos *(GDPR)*, **las empresas, incluyendo a los autónomos y a las organizaciones benéficas, deben permitir el acceso fácil a los datos que son guardados sobre las personas y también deben obtener el consentimiento de las personas sobre las cuales quieren recopilar datos.**
¿Qué significa eso para tu negocio? Bueno, **los boletines informativos y otros métodos de marketing por correo electrónico deben pedir EXPRÉSAMENTE a los destinatarios que se suscriban y los clientes deben aceptar el uso de cookies y el seguimiento en línea**. Esto también requiere que todos los datos sean recopilados y almacenados por razones legitimas y solo se guarden durante el tiempo que sea necesario.
Y esto no va solamente de políticas de protección de datos. Las organizaciones que cumplen con los requisitos también **deben contar con sistemas técnicos para asegurar la protección de datos.**

El papel de los sistemas informáticos y el almacenamiento de datos en la gestión del riesgo

Incluso si una empresa ha cumplido con los requisitos para obtener el consentimiento de las personas, **su obligación solo se cumple si los datos están seguros, con todo lo que ello supone.** Y no solo nos referimos a la protección contra los cibercriminales. **Los datos también deben ser protegidos contra otros empleados** y personas que toman decisiones dentro de una organización.
Para protegerlos, asegúrate de **revisar constantemente las autorizaciones y los niveles de acceso de los empleados** *(uno de los principales vectores de ataque)*. También debes tener cuidado y **elegir contraseñas seguras y diferentes para cada servicio**.
Si tienes un servidor físico, asegúrate de tener **un hardware confiable** que incluya cables de alimentación y de

datos *(ES)* de buena calidad *(que luego vienen las sorpresas)*, así como **un software que garantice el cifrado**. **Si almacenas tus datos en una nube** a través de un tercero,**confía solamente en las empresas que se comprometen con la obligación legal de informarte sobre cualquier fallo de seguridad** que pueda haber en sus sistemas. Y por supuesto, que cuenten con sistemas que cumplan la legislación que te compete. La GDPR se ha vuelto en este escaso año ya casi un estándar de la industria, pero por si acaso, asegúrate que en efecto ese proveedor de servicio cuenta con las medidas de seguridad adecuadas para que tu cliente pueda ejercer los derechos que contempla esta regulación.

Si bien puede ser difícil navegar por la evolución de las normas y regulaciones del procesamiento de datos, es crítico caer en la consideración de que no nos queda más remedio que ser proactivos a la hora de entender y respetar los principios básicos, incluyendo la protección de la privacidad, la transparencia y la debida diligencia en el almacenamiento de datos.
Ya no solo por las multas que nos van a caer si algo pasa, sino también por la crisis reputacional a la que nos vamos a enfrentar, e incluso por todo lo que puede suponer a nivel de nuestro negocio que algo así acabe ocurriendo.



Fuente de información:
https://retina.elpais.com/