"La nueva normativa de protección de datos y los sistemas de compliance."

Las organizaciones se han visto obligadas a revisar su modelo de control interno de datos

5D

CARLOS ALBERTO SÁIZ PEÑA

Getty Images

Compatir en FacebookCompatir en TwitterCompatir en LinkedinEnviar por correo Ir a comentarios

Madrid 16 ENE 2019 - 09:12 CET

El 6 de Diciembre de 2018 se publicó la ya conocida como LOPDGDD, o Ley Orgánica de Protección de Datos y Garantía de Derechos Digitales, que viene, por un lado, a complementar el Reglamento Europeo de Protección de Datos (RGPD), y por otro lado a reconocer una serie de derechos digitales a los ciudadanos entre los que mencionaremos especialmente los relativos al ámbito laboral.

Sin duda, la normativa de protección de datos ha sido uno de los principales marcos normativos que se han incorporado en los Sistemas de Compliance globales de las compañías en los últimos años y precisamente de este tema –entre otros muchos- hablaremos junto a Mar España, directora general de la Agencia Española de Protección

de Datos, en el próximo Encuentro de Cumplen (Asociación de Profesionales de Cumplimiento Normativo), los próximos 24 y 25 de enero en el Casino de Madrid.

Y es que tener dos normas tan relevantes como el RGPD y la LOPDGDD, y la aparición de la figura de los DPO (Data Protection Officer o Delegados de Protección de Datos) han obligado a todo tipo de organizaciones a revisar su modelo de control interno de datos y configurarlo conforme a nuevos principios como enfoque a riesgos, privacidad en el diseño y responsabilidad proactiva.

Merece la pena destacar varias ideas sobre el impacto de la normativa de protección de datos, y especialmente la LOPDGDD, en los sistemas de compliance corporativos:

- Se tipifican las infracciones en un amplio listado, diferenciando 3 niveles: leves, graves y muy graves. Por ello las organizaciones ya pueden incluir en sus métodos de cálculo de riesgos normativos los diferentes impactos que podría tener un incumplimiento concreto.

- Se definen la tipología de organizaciones que necesitan nombrar a un DPO. Esta figura ha ido recayendo en diferentes perfiles dentro de las organizaciones, pero precisamente existen bastantes casos donde DPO y Compliance Officer son la misma persona, o el primero depende del segundo como un área funcional.

- Se trata de una normativa cuyo contenido va muy alineado con la forma de trabajar de las áreas de compliance tradicionales (cálculo de riesgos, definición de medidas de prevención, detección y reacción, verificación de cumplimiento, formación y creación de una cultura de cumplimiento, existencia de un entorno sancionador importante, etc.

- El éxito de un buen sistema de protección de datos personales dependerá, en gran medida, de la capacidad de conocer con antelación y asesorar debidamente sobre las diferentes actividades de tratamiento de datos que se lleven a cabo en la organización, o como suele decirse, "estar pegado al negocio". Este criterio viene aplicándose a los sistemas generales de Compliance como una idea base desde hace tiempo.

- En la LOPDGDD se regulan en el artículo 24 los sistemas de información de denuncias internas, más conocidos como canales de denuncia. El artículo permite que las denuncias sean anónimas y regula además diferentes plazos de conservación de la información, así como los derechos que se deben respetar de denunciante y denunciado en relación con el tratamiento de sus datos.

- Asimismo, se regulan diferentes derechos digitales de los trabajadores en el ámbito laboral (uso de dispositivos, desconexión digital, videovigilancia, geolocalización) que resulta necesario conocer por la empresa y establecer los protocolos adecuados para respetarlos y no vulnerar la intimidad de los trabajadores en las tareas de monitorización y establecimiento de controles proporcionados.

Como conclusión, el respeto por la privacidad y la ética digital son una necesidad cada vez más relevante para las empresas, especialmente aquellas que siguen trabajando en su transformación digital. Las brechas de seguridad, el robo de datos o el uso indebido de información de clientes o empleados no sólo pueden implicar severas multas por la autoridad de control a la empresa, sino también una pérdida de confianza en el mercado y un daño reputacional de enorme impacto. En todo caso, resultará fundamental la adopción de medidas de control para cumplir con el RGPD y la LOPDGDD coherentes con el Sistema global de Compliance de la organización de cara a ser más eficientes y mitigar mejor los riesgos reales de la organización.

Carlos Alberto Saiz Peña Socio de Ecix Group Presidente de CUMPLEN (Asociación de Profesionales de Cumplimiento Normativo).