El Reglamento General de Protección de Datos (GDPR) de la Unión Europea y sus implicaciones en México

Category: Data Protection,Firm news
written by Nader, Hayaux & Goebel | junio 30, 2021

Los avances tecnológicos exponenciales vistos en las últimas décadas, en particular el uso de big data y servicios digitales, potencializado por la nueva dinámica impuesta por la emergencia sanitaria derivada de la pandemia, han puesto mucha presión en la regulación de protección de datos personales, lo que ha hecho que las autoridades a nivel global se cuestionen si se requiere un régimen de protección más estricto.

En esta tendencia, el 25 de mayo de 2016, la Unión Europea emitió el Reglamento General de Protección de Datos ("GDPR" por sus siglas en inglés). El GDPR abrogó la Directiva de protección de datos (Directiva 95/46 /CE) de 1995 de la Unión Europea (la "UE") (la "Directiva de la UE"), con el objetivo de reforzar la regulación en materia de protección de datos personales.

El GDPR es obligatorio para: (i) entidades establecidas en la UE, y (ii) entidades que encontrándose fuera de la UE, ofrezcan y dirijan sus productos o servicios a ciudadanos de la UE.

México, basándose en los principios de la Directiva de la UE, publicó el 5 de julio de 2010, la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, y posteriormente, su regulación secundaria (la "Ley de Datos").

La Ley de Datos no ha sido homologada al GDPR; sin embargo, las personas y sociedades mexicanas podrían estar obligadas a cumplir con el GDPR en caso de que (i) ofrezcan y entreguen productos o servicios de manera habitual a habitantes de la UE, o (ii) utilicen herramientas que les permitan rastrear cookies o direcciones IP de

personas que visiten su sitio web desde países de la UE.

En caso de incumplimiento, las personas o entidades mexicanas, o sus filiales en la UE, podrían estar sujetas a sanciones bajo el GDPR. Las multas pueden ser de hasta €20 millones o 4% del volumen de facturación anual. Durante los tres años de vigencia del GDPR, la Comisión Europea ha impuesto 680 multas, que suponen más de 287 millones de euros.(1)

La Ley de Datos y el GDPR comparten principios sustancialmente iguales:

1. La obligación de obtener el previo consentimiento del titular para el tratamiento de sus datos personales;
2. La obligación de contar con un aviso de privacidad, y ponerlo a disposición del titular previo al tratamiento de sus datos;
3. La facultad del titular para ejercer sus derechos de Acceso, Rectificación, Cancelación y Oposición (los "Derechos ARCO");
4. Los conceptos de (i) responsable, quien es la persona que decide sobre el tratamiento de los datos personales del titular, y (ii) el encargado, quien es la persona que trata los datos personales del titular por cuenta del responsable; y
5. La obligación de designar a un delegado de protección de datos (DPO), quien será el encargado de supervisar el cumplimiento de la regulación.

Algunas de las obligaciones que incorporó el GDPR, que no están previstas aún en la regulación mexicana, son:

1. El derecho a la portabilidad, el cual faculta al titular a obtener una copia de sus datos personales tratados por el responsable;
2. Introduce el principio de protección de datos desde el diseño (Privacy by Design);
3. Establece obligaciones expresas respecto del consentimiento de un niño menor a 16 años; y
4. Obligaciones y requisitos nuevos en caso de que el responsable utilice tecnologías novedosas en el tratamiento de datos.

Como sugerencia, las Entidades mexicanas que puedan obtener y tratar datos de

residentes de la UE o las subsidiarias mexicanas de empresas internacionales, deben analizar el impacto del GDPR en sus operaciones en México, y considerar fortalecer su régimen de protección de datos personales, para cumplir con los estándares internacionales, incluyendo el GDPR, para evitar contingencias y multas.

The General Data Protection Regulation (GDPR) of the European Union and its implications in Mexico

The exponential technological advances in recent decades, in particular the use of big data and digital services, enhanced by the new dynamics imposed by the health emergency derived from the pandemic, have stressed the current regulation on personal data protection, which has led authorities worldwide to question whether a stricter protection regime is required.

At the head of the trend, the European Union adopted on May 25, 2016, the General Data Protection Regulation ("GDPR"). The GDPR repealed the 1995 European Union (the "EU") Data Protection Directive (Directive 95/46 /EC) (the "EU Directive"), with the purpose to provide more strict regulation regarding the protection of personal data.

The GDPR is mandatory for: (i) entities established within the EU, and (ii) entities resident outside the EU, which offer their products or services to EU citizens.

Mexico, following the principles of the EU Directive, published on July 5, 2010, the Federal Law for the Protection of Personal Data in Possession of Individuals, and subsequently, the secondary regulation (the "Data Law").

The Data Law has not been homologated to the GDPR; however, Mexican individuals and companies may be required to comply with the GDPR if (i) they offer and deliver products or services on a regular basis to EU residents, or (ii) they use tools that allow them to track cookies or IP addresses of people visiting their website from EU countries.

In case of breach, Mexicans individuals or entities, or their affiliates located in the EU, may be subject to penalties under the GDPR. Fines can be up to €20 million or 4% of the annual revenue. During the three years in which the GDPR has been in

force, the European Commission has imposed 680 fines, amounting to more than €287 million.

The Data Law and the GDPR share substantially the same principles:

1. The obligation to obtain the prior consent of the owner for the processing of his/her personal data;
2. The obligation to have a privacy notice and to deliver it to the owner prior to the processing of his/her data;
3. The terms in which the owner may exercise his/her rights of Access, Rectification, Cancellation and Opposition (the "ARCO Rights");
4. The incorporation of the concepts of (i) the data controller (Responsable), who is the person that decides on the processing of the personal data of the owner, and (ii) the data processor, who is the person that process the data on behalf of the data controller; and
5. The obligation to appoint a Data Protection Officer who will be in charge of supervising compliance with the regulation.

Some of the new obligations incorporated by the GDPR, which are not included yet in the Mexican regulation, are:

1. The portability right, which entitles the owner to obtain a copy of his/her personal data processed by the Controller;
2. Introduces the principle of data protection by design (Privacy by Design);
3. Incorporates express obligations regarding the consent of minors under 16 years of age; and
4. New obligations and requirements if the data controller implements new technologies in the processing of the data.

As a suggestion, Mexican companies that might obtain and treat data from EU residents or Mexican subsidiaries of international companies, must evaluate the impact of the GDPR in their operations, and consider strengthening their personal data protection regime to comply with international standards, including the GDPR, to avoid any contingencies or fines.

(1) GDPR Enforcement Tracker al 2021;

https://www.enforcementtracker.com/?insights

Para mayor información sobre el GDPR y el régimen de protección de datos personales en México, nos ponemos a sus órdenes con sus contactos habituales en Nader, Hayaux & Goebel.

Luciano Pérez Gómez

+52 (55) 4170 3027

lperez@nhg.com.mx