大成 DENTONS MUÑOZ

Is your business ready for the GDPR, Europe's new data protection legislation?

What is the GDPR?

The EU General Data Protection Regulation (GDPR)[1] overhauls the legal framework related to the handling and processing of personal data by companies.

The GDPR is effective May 25, 2018. The GDPR essentially seeks to establish greater protection for the personal data of EU residents by requiring companies and public authorities to comply with stricter requirements. These requirements relate to legal bases for the processing of personal data, the rights of data subjects (e.g., the "right of erasure"), cross-border data transfers, the safekeeping of data, data breach notifications and other matters.

We have no subsidiaries or direct business operations in Europe, does GDPR affect us?

YES, the GDPR is global in its effect, and may apply to any Central American company that processes the personal data of EU residents.

A large number of companies with no direct operations in the EU are still affected by the GDPR.

One of the most significant changes resulting from the GDPR is the broadening of the territorial scope of the relevant legal framework. The GDPR envisages two circumstances in which organizations not established in the EU would be subject to its provisions:

(1) Where the personal data of EU residents is being processed "by a controller or a processor not established in the Union" and "the processing activities are related to offering goods or services to such data subjects irrespective of whether connected to a payment"[2]

(2) Where the personal data of EU residents is being processed "by a controller or processor not established in the Union" and processing "is related to the monitoring of the behaviour of such data subjects as far as their behaviour takes place within the Union"[3]

Therefore, the GDPR may apply to Central American organizations even where they are not engaged in any business transactions with EU entities or consumers.

[1]Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/.
[2]Article 3 (2) (a) and Rec. 23, GDPR.
[3]Article 3 (2) (b) and Rec. 24, GDPR.

Based on the further provisions of the GDPR, the monitoring scenario, in particular, could capture a number of organizations with a web presence that may be deemed to track a natural person "in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes."[4] Organizations from outside the EU that fall under the GDPR are obliged to appoint a representative (acting as a point of contact) in the EU unless their processing is occasional, does not include a large scale of sensitive data and is unlikely to result in a risk to the rights of natural persons.

What are the consequences of noncompliance with the GDPR?

The consequences of noncompliance are wide-ranging. The maximum fine is the greater of either four percent of annual worldwide turnover or €20 million.

The nature, gravity and duration of any infringement or noncompliance will be decisive in any relevant supervisory authority's decision to impose a fine. Supervisory authorities may also require certain remedial actions to be undertaken by noncompliant organizations, instead of or in addition to fines.

What are the principal provisions of GDPR?

- **Legal bases:** Data processing must be founded on one of the following six legal bases: Consent, overriding legitimate interest, performance of contract, legal obligation, vital interest of the data subject and public interest.
- **Data protection principles**: Companies must be able to demonstrate compliance with the principles of data minimization, purpose limitations and accuracy.
- **Transparency (duty to inform)**: The GDPR increases the information you need to include in your privacy notices. They must be concise and legible.
- **Right of data subjects**: Subjects must have access to their personal data and the ability to demand its deletion and portability on request. All requests must be fulfilled within 30 days. A company's request-handling policy should be introduced with its template responses.
- **Documentation**: Companies must keep certain internal records, but are no longer required to notify data protection authorities of data protection activities.
- **Employment relations**: Companies must update employment contracts and notices to employees to comply with the GDPR.
- **Outsourcing**: Certain stringent obligations must be contained in contracts with data processors (e.g., mandatory audit).
- **Cross-border data transfer**: The GDPR prohibits transfer of personal data outside the EU unless certain conditions are met.
- **Automated decision-making processes, including profiling**: Individuals must have the right to opt out.
- **Data Protection Impact Assessment**: Might be required where "high-risk" processing is carried out.
- **Data breach notification**: Data must be kept secure and data breaches must be recorded and notified to the supervisory authority (unless the breach is unlikely to be a risk for individuals) within 72 hours.
- **Data security / privacy by design, by default**: Companies are required to implement appropriate technical and organizational measures, both at the time of determination of the means for processing and at the time of the processing itself. Any such privacy-by-design measures may include, for example, pseudonymisation or other privacy-enhancing technologies.
- **Governance / Data Protection Officer (DPO) / representative**: Depending on the processing you carry out, you may need to appoint a DPO. DPOs cannot be dismissed or penalized for performing their role.

For more information, or if you have any questions, please email monserrat.guitart@dentons.com

[4] Ibid.

ABOUT DENTONS

Dentons is the world's largest law firm, delivering quality and value to clients around the globe. Dentons is a leader on the Acritas Global Elite Brand Index, a BTI Client Service 30 Award winner and recognized by prominent business and legal publications for its innovations in client service, including founding Nextlaw Labs and the Nextlaw Global Referral Network. Dentons' polycentric approach and world-class talent challenge the status quo to advance client interests in the communities in which we live and work.

dentons.com

CSBrand-8838_GDPR-alert-for-US-businesses-07 — 25/05/2018