17th May 2017

Informative release

Is your company prepared for the GDPR?

The new GDPR comes into force on the **25th of May 2018**. Any company which is not in compliance with this rule by that date, will afford the largest of these fines: **20M Euro or 4% of the annual international turnover** of the company.

Any company, European or not (if it renders its services to EU citizens) which access to any kind of PII, shall implement the organizational and technical measures required to comply with the new obligations set forth in Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regards to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC ("**GDPR**") which comes into force on **25 May 2018.**

The main highlights of the GDPR are summarized as follows:

- **Application to Controllers and Processors located Outside the EU** whose flows of personal data are from and to countries outside the EU. In some cases, operators located outside the EU will need to appoint a representative within the EU.

- **Increase of Fines**: Under the GDPR fines could amount up to 4% of annual worldwide turnover and € 20 million.

- **Requirement of Explicit Consent:** Consent must be "explicit" for sensitive data. The data controller is required to be able to demonstrate that consent was given.

- **Previous Processing Notice:** Data controllers must continue to provide transparent information to data subjects when personal data are collected.

- **New Rights in Favour of Data Subjects:** These include "data minimization", "data portability" and "right to be forgotten".

- **New Obligations for Data Processors**, such as, maintain records of processing activities under its responsibility, cooperation with the supervisory authority and make those records, on request, available to it, appoint a data protection officer and notify the controller any data breach.

- **Data Breach Notification**: Data controllers must notify serious data breaches to the relevant data protection authority not later than 72 hours after having become aware of it.

- **Principles of Data Protection By Design and Data Protection By Default:** Such measures could consist, inter alia, of minimizing the processing of personal data, pseudonymising personal data as soon as possible, transparency in regards to the functions and processing of personal data, enabling the data subject to monitor the data processing, enabling the controller to create and improve security features.

- **Principle of One-Stop-Shop:** Any company located outside EU only has to deal with one data protection authority.

- **Binding Corporate Rules:** The GDPR expressly recognizes Binding Corporate Rules for controllers and processors as a means of legitimizing intra-group international data transfers.

- **International Transfers:** Prior authorization shall be exempted in case of international data transfers based on approved safeguards such as Commission or DPA approved contracts.

- **Data Protection Officer**: Most of the companies which relevant volumes of data flows or a significant size shall have to appoint a data protection officer ("DPO"). The DPO may be an employee or under a service contract.

In **Andersen Tax and Legal**, we have an extensive experience adapting companies of all industries to GDPR. We also offer DPO services in an outsourcing basis.

The **Privacy, IT & Digital Business** area is composed by a large group of professionals specialized in data protection, GDPR compliance and new technologies, amongst other topics.

Main Professionals:

Natalia Martos Díaz
Partner
natalia.martos@AndersenTaxLegal.es

Isabel Martínez Moriel
Senior Lawyer
isabel.martinez@AndersenTaxLegal.es

María García Zarzalejos
Lawyer
maria.gzarzalejos@AndersenTaxLegal.es

For further information visit Privacy, IT & Digital Business.