Informative Note

When is it necessary to appoint a Data Protection Officer? In the wake of the first sanction by the Spanish Data Protection Agency

26th July 2020

The appointment of a DPO is not mandatory for all companies, although it is advisable to have a DPO in any organization that handles a significant amount of personal data

Following the recent decision of 10th June 2020 by the Spanish Data Protection Agency (AEPD) against Glovo, which was the first sanction imposed on a company in Spain for not having appointed a data protection officer (DPO), many organisations are wondering whether they are incurring a similar risk.

It should be borne in mind that, although the amount of this penalty was not very high (i.e. 25,000 euros), the fact of having infringed current data protection regulations automatically makes an operator a repeat offender in subsequent penalty proceedings. Therefore, in the event of a new breach, the risk of penalty is compounded by the possibility of suffering the imposition of an aggravating circumstance (which increases the amount of the penalty). Furthermore, in any case, since the decision to impose a penalty is public, the offending companies assume a reputational risk that may have repercussions on their business, since both customers and public administrations increasingly demand guarantees of full compliance with the data protection regulations prior to any contract in order to avoid the transmission of any legal risk.

It should be noted that the figure of the DPO is new, since it has been created by the General Data Protection Regulation (RGPD), which came into force in May 2018. Therefore, it is a figure that may go unnoticed, although it is becoming increasingly important as data-based business models increase.

The DPO is, to a large extent, the person in charge of supervising compliance with data protection regulations within your organization, analysing all projects, technologies and systems that involve the processing of personal data. Therefore, despite exercising an internal role vis-à-vis the company, it is important to guarantee its full independence and freedom. In addition, the DPO is also responsible for responding to and dealing with requests and applications from data subjects, and for liaising with the relevant supervisory authority. For all these reasons, it is essential that the DPO has advanced knowledge of data protection.

On the other hand, it should be noted that the appointment of a DPO is not mandatory for all companies, although it is advisable to have a DPO in any organization that processes a significant amount of personal data, in order to ensure proper processing of personal information within the organization.

In general, the RGPD establishes two large groups of obligated parties whose interpretation is open:

- Organisations whose main business activities involve the processing of sensitive data, on a large scale or involve the regular and systematic monitoring of individuals on a large scale.

- Public authorities or bodies, except courts.

In Spain, the Organic Law 3/2018 of 5th December on Data Protection and Guarantee of Digital Rights (LOPDGDD) specifies that, within these broad categories, entities in certain sectors are in any case obliged to do so. Without being exhaustive, we summarize these cases:

- Teaching centres that offer education at any of the levels established in the legislation regulating the right to education, as well as public and private universities (this is always regulated education - not centres with their own or private degrees that are not officially recognised).

- Credit entities and financial credit establishments.

- Insurance and reinsurance entities.

- Investment services companies, regulated by the Stock Market legislation.

- Operators that carry out the activity of gaming through electronic, computer, telematic and interactive channels, in accordance with the regulations governing gaming.

- Entities that develop advertising and commercial prospecting activities, when they carry out activities that imply the elaboration of profiles of the same.

- Entities operating networks and providing electronic communication services, when they habitually and systematically process personal data on a large scale.

- Information society service providers when they produce large-scale profiles of service users.

- Entities responsible for common files for the evaluation of creditworthiness or common files for the management and prevention of fraud

- Electrical energy distributors and marketers and natural gas distributors and marketers

- Sports federations when they process data on minors.

- Professional associations and their general council.

- Health centres that are legally obliged to keep patients' medical records, except for health professionals working on an individual basis.

Although the work of specifying the LOPDGDD is appreciated, determining whether a company is in one of these cases may also require some work on the interpretation of undetermined legal concepts, such as "large-scale data processing" or "user profiling", which makes it advisable to have specialized legal advice.

Andersen's Privacy, IT & Digital Business Area has a highly specialized and qualified team in data protection and advisory services in the functions of DPO or support to the designated DPO, under the maxims of excellence, commitment, responsibility and professionalism.

For more information please contact:

Isabel Martínez Moriel

isabel.martinez@es.andersen.com