"GLOVO" IS FINED IN SPAIN WITH €25,000.00, DUE TO A DATA PROTECTION MATTER... WHAT WILL THIS CASE LOOK LIKE IN PANAMA?

BY PUBLIO CORTÉS

Weeks ago, the Spanish Data Protection Agency (AEPD for its acronym in Spanish) set a fine of €25,000.00, that is, approximately US $ 29,695.00, within Procedure No.: PS/00417/2019, against the legal entity that operates GLOVO in Spain, for not have appointed the "Data Protection Officer" who, according to the agency, should have been appointed according to the legislation that governs Spain. The media report that this is the first time that a fine of this kind has been imposed in said country. The highest fine ever at the European Union (EU), for this same issue was against FACEBOOK applied in Germany, for an amount of €51,000.00, approximately US $ 60,577.54

Although it has been published that the administrative decision will be subject to a motion to review, we find it extremely useful to analyze the ruling, as it was issued by the AEPD and later, question ourselves of what could happen in Panama in a similar situation, but under the framework of Law 81 of 2019 "Personal Data Protection", which will come into effect in March 2021.

General Sketch of the Legal Framework in Spain

Spain is a member of the EU and for starters, Regulation (EU) 2016/679 of the European Parliament and of the Council, known in Spain by the acronym GDPR ("General Data Protection Regulation") applies thereof, and its incorporation into the Spanish legal system was made through Organic Law 3/2018, on Personal Data Protection and Guarantee of Digital Rights, known by the Spanish acronym LOPDGDD. There are three roles defined within a company in the GDPR under the terms of data protection and relate to the mentioned case, namely:

"Controller" or "Responsible person": "the natural or legal person, public authority, service or other body that, alone or together with others, **determines the purposes and means of processing [of the data]**"; (The highlight is ours).

"Processor": "the natural or legal person, public authority, service or other body **that processes personal data on behalf of the controller [of the data]**" (The underlying is ours); and

"Data Protection Officer": Person designated by the Controller and the Processor, who has the following tasks:

a) "Inform and advise the person in charge or the Processor and the employees who manage data, of the applicable obligations thereof, upon them under this Regulation and other data protection provisions of the Union or that of the Member Nations;

b) Monitor compliance with the provisions of this Regulation, other data protection provisions of the Union or that the Member Nations and the policies applicable to the controller or processor regarding personal data protection, including the assignment of responsibilities, awareness and training of the personnel participating in processing operations, and the corresponding audits;

c) Offer the required assessment regarding the impact evaluation related to data protection and supervise its application in accordance to article 35;

d) Cooperate with the supervisory authority;

e) Act as the contact point of the supervisory authority for questions related to the processing, including the prior consultation referred to in article 36, and carry out consultations, where appropriate, on any other matter."

The European Regulation provides that

there should **not always** be a "Data Protection Officer". There are only three (3) cases in which their appointment is necessary. One of these assumptions is under discussion in the aforementioned case and is the one that requires the Officer to be appointed when: “the main activities of the controller or processor consist of [data] processing operations that, due to their nature, reach and/or purposes, **require a regular and systematic observation of large-scale stakeholders**,” (The emphasis is ours).

There is an open discussion in Europe as to what is meant by “large-scale” data processing. Some domestic legislation define it, others do not. As for the LOPDGDD, it provides that the designation of the "Data Protection Officer" must be made in the cases provided by the GDPR and it also indictes that the authorities must be informed within the following 10 days.

The process on the case of the “GLOVO” fine

As described by the ruling whereas the fine was imposed, the basic ritual of the process was as follows:

(1) Two people, on different dates (May and November 2019), filed claims against GLOVO for not having designated the "Data Protection Officer".

(2) GLOVO is notified whose response is, that it is not within the scope of the GDPR or the LOPDGDD, and thus, it does not feel obligated to designate a "Data Protection Officer".

(3) The AEPD begins the process on January 13, 2020, where GLOVO filed allegations with the defense argument set forth above, adding that it appointed a Data Protection Committee and a Subcommittee that performed the same tasks that the GDPR establishes for the “Data Protection Officer”.

(4) An administrative case is opened to a probation stage, after which the AEPD presents a proposal for a sanctioning resolution.

(5) The draft ruling was the subject of a final statement by GLOVO, on March 13, 2020, in which it states that since May 2019 it had appointed a person as "Data Protection Officer", but that this was not formalized by notification to the AEPD, until February 2020. However, they insisted that before that, the legitimate rights and freedoms of those interested in the data had been protected because the Data Protection Committee, the Subcommittee and the Legal Department, had been fulfilling their tasks as "Data Protection Officer".

The Decision to Fine

The AEPD considers as proven facts, that GLOVO did not appoint the "Data Protection Officer"; that the company claims

that it is exempted from the obligations of the appointment of said Officer regulated in both European and domestic level, although it says that with the Data Protection Committee appointed, the tasks of the Officer were already taken care of; and, finally, that on January 31, 2020, GLOVO notified the AEPD of the appointment of the “Data Protection Officer”, which took place after the beginning of the sanctioning procedure, which occurred on January 13, 2020.

According to the AEPD, these facts are within the regulations of the GDPR and the LGPDGDD that we have previously mentioned, and it concludes that GLOVO should have appointed the "Data Protection Officer", because it understands that the activity of this company consists of the processing of data whose nature, scope and / or purposes require a regular and systematic observation of the data subjects on a large scale. It also emphasizes the fact that, when the sanctioning process began, the GLOVO website was verified and the existence of the “Data Protection Officer” was not mentioned.

Finally, it analyzes the sanctioning jurisdiction and the applicable sanction regulations for non-compliance with the duty of designation of the "Data Protection Officer", condemning the payment of the fine we are referring to, clearly establishing the notification mechanisms and resources that the affected party may use.

What would happen in Panama?

In simpler words, the "Data Protection Officer" to which the effective GDPR refers to, is some sort of a "Compliance Officer" who supervises within the company, compliance with the regulations and data protection policies and liaises with the supervisory authority.

In this European scope, it is not mandatory to have that executive appointed in all cases, however, when

the company has to process data from interested parties or data holders "on a large scale", it is necessary to have a "Data Protection Officer" and the authority is informed about their appointment.

Assuming that Law 81 of 2019 were to be in enforced, since it is a legal person who operates a digital platform for commercial purposes, GLOVO would be governed by this Law in Panama.

However, the most important comment we can make is that, said Panamanian Law does not have a figure with a role that is equivalent to the "Data Protection Officer" of the European GDPR. Neither with that name nor under another name, therefore, the debate on the cases in which that executive should be appointed, would not even be a topic for discussion in Panama. The entity that operates GLOVO in Spain would not be fined if it operated in Panama.

Our Law does contemplate the roles of the "Responsible for Data Processing", very similar to the European "Controller", and of the "Custodian of the Database", whose role is equivalent to that of the European "Processor". However, we want to emphasize, that it does not impose the appointment in any company of a "Data Protection Officer" or similar.

Anyway, let us make other comparisons of the case with the Panamanian regulation:

- The supervisory authority in Panama is the National Authority for Transparency and Access to Information (ANTAI) with technical support from the Government Innovation Authority (AIG). For this supervisory work, the Law does not speak of a specific link within the company in the form of a "Compliance Officer", therefore, the "Responsible" and "Custodian"

should practice playing this role, in general terms.

- The Law contemplates some elements of the sanctioning procedure, for example, that an ANTAI Directorate sets the fines, when applicable, that it is subject to a “Motion to Reconsideration” before said Directorate and an appeal before the highest authority of ANTAI. However, the details of the procedure refer to the regulation that is still pending to be issued.

- To state the obvious, there is no conduct in Panama that is to be considered a "misdemeanor" due to the non-appointment of an official equivalent to the European "Data Protection Officer".

- The monetary fines in Panama for "serious" and "very serious" offenses are less burdensome: minimum US $ 1,000.00 and maximum US $ 10,000.00. Of course, in the case of "very serious", the data processing may be closed, temporarily or permanently, with the support of the Police in executing the measure.

FINAL COMMENTS

We take this opportunity to mention that we are few months away for the Law 81 of 2019 "On Personal Data Protection" enters into full effect in Panama and to this date it still has not been regulated, although it needs to be. This does not prevent its enforcement, but it complicates its application quite a bit. Although this Law does not apply to subjects regulated by special laws, when said laws meet the minimum data protection standard, it is a fact that there are many subjects that will be governed by this new regulation and as a country we have a year and months of delay in the task of regulation.

Likewise, it is important that the mandate of said Law be fulfilled, which promises that ANTAI will have the necessary budgetary resources to fulfill the tasks assigned to it, under Law 81.

Despite the lack of regulations and the uncertainty on whether or not ANTAI will have the resources to carry out its tasks, it is essential that organizations prepare to fulfill the duties that the Law imposes on them. There are only a few months left.

International standards of interaction in the digital world require a high level of respect and security in the processing of data of interested parties or holders, whether they are national or alien. Even more so now, when the economic crisis derived from COVID-19, has greatly enhanced digital interaction and electronic commerce. No country can afford not to comply with these standards, which involve, not only the existence of standards, but also a real and effective compliance monitoring system.

Explore our Legal Bulletins Collection at www.legaladvisorpanama.com

PUBLIO CORTÉS
ABOGADO - LAWYER

WWW.LEGALADVISORPANAMA.COM

M: +507 6679-4646 E: CORTES@LEGALADVISORPANAMA.COM

@PUBLIOCORTES.LAWYER