PETERKA PARTNERS

THE CEE LAW FIRM

While the amendments to the Bulgarian Data Protection Act are still pending, sanctions imposed for non-compliance with the GDPR are already a fact

Until recently, there was a popular but unfounded belief in some parts of the business community that no penalties for violations of the GDPR[1] would be imposed before the amendments to the local Data Protection Act come into force. However, a newly published Decision[2] of the CPDP[3] has put those rumours to rest. For the sake of clarity, it should be noted that indeed implementation of the GDPR into Bulgarian legislation is not a prerequisite for the imposition of sanctions by the local data protection watchdog.

In a nutshell, the Decision discussed in this article is based on a complaint by a data subject. A Bulgarian bank used data obtained by a data subject in the course of a contractual relationship (for signing and performing a loan contract) to later contact the same data subject with a request for information about a third person.

The CPDP imposed a fine amounting to BGN 1,000 (approximately EUR 500) which seems to be the lowest fine yet imposed by a supervisory authority for GDPR violation. For reference, Google was fined EUR 57 million by the French data protection authority, a fine of EUR 150,000 was imposed on a hospital in Portugal, etc. However, no meaningful parallels can be made as not all of the details of these cases are publicly available.

The aim of this article is to share our initial thoughts on the said Decision in view of the CPDP's approach when applying the GDPR and imposing penalties for violations of it. Thus, we would like to touch upon the following points:

Personal data should be processed only for specified, explicit purposes

The processing of personal data for any other purpose incompatible with the initially specified purposes disclosed to the data subject when the personal data were obtained is likely to be considered by the CPDP as a violation of one of the main principles of the GDPR. Thus, it is essential for data controllers to identify correctly the purposes for the processing of each data category at the point of collection of these data. Otherwise, the processing may turn out to be unlawful.

Various factors are considered by the CPDP when deciding on sanctions

Basically, the nature and duration of the breach, as well as the number of data subjects affected seem to be among the main factors taken into consideration by the CPDP in the decision-making process. At the same time, the lack of material damages and the fact that no special categories of personal data have been affected can be seen as extenuating/mitigating circumstances which can lessen the impact of the violation.

On the other hand, it seems that not all violations result in a fine though. For another breach committed by the same bank according to the Decision in question, i.e., violation of the data subject's right of access, the Bulgarian supervisory authority simply instructed the data controller to provide all of the necessary information as per the requirements of the GDPR.

---

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 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/EC (General Data Protection Regulation).

[2] Decision No. PPN-01-111/2018 dated 04.12.2018.

[3] Commission for Personal Data Protection.

Ambiguous information to data subjects may result in non-compliance

While not explicitly defined in the GDPR, transparency takes the form of specific practical requirements on data controllers and processors. The Bulgarian supervisory authority seems to apply a rather strict interpretation of these requirements. In particular, the CPDP considered the general statement that the personal data were disclosed to "data processors" not enough to fulfil the controller's obligation to provide information on the recipients/categories of recipients to whom the personal data have been or will be disclosed. In view of that understanding, it may be a good idea for both data controllers and data processors to consider rewriting any rather vague phrases used in their privacy policies and/or standardized answers to data subjects' requests.

What is to be understood by "direct marketing"

Even though the amendments to the local Data Protection Act are still pending before the National Assembly, we can see from the draft act that the latter plans to revoke the currently applicable definition of "direct marketing". Thus, any decisions, statements or instructions where the local supervisory authority elaborates on the meaning of this term are more than welcome.

Based on the wording of the Decision, it seems that at least for the time being the CPDP generally sticks to the definition of "direct marketing" applied so far. Nevertheless, it appears that the supervisory authority further develops the definition by adding to it also the popularization of a company's activity, including sending of information about its services or promotions, as a type/variation of direct marketing.

In light of the Decision's elaboration on direct marketing, another interesting point is that a data subject's application for erasure of his/her personal data is not interpreted by the CPDP to be equal to an objection against processing for direct marketing purposes. Given that, as we see it, provided there is a valid legal basis for the processing, the data controller is not obliged to stop the processing of personal data for such purposes unless an explicit request in this regard is at hand.

Personal data may be stored even after the statutory periods have expired

The Decision outlines that, in general, data controllers/processors may continue processing a data subject's personal data after the contractual relationship between them is terminated, provided there is a statutory obligation to do so (for example, for anti-money laundering purposes, accounting, etc.). In addition to that, the CPDP basically confirms that data can be further processed after the statutory terms have expired if based on a legitimate interest of the controller to defend itself against possible legal claims by the data subject. However, it should always be considered on a case-by-case basis whether the retention period is "proportionate" to the statutory obligations and to the legitimate interests for processing.

Awaiting new rulings

Considering that not all of the CPDP's decisions are publicly available, it is not clear whether this is the first case of a fine for GDPR violation imposed in Bulgaria. As announced by the CPDP, more than 800 complaints for personal data breaches have been submitted in 2018 – about 600 of which after the GDPR became applicable. This goes to show that the Bulgarian supervisory authority's interpretation of the GDPR remains to be seen. So, stay tuned.

* * *

The article was prepared by Mr. Georgi Kanev, Senior Associate and Deputy Director, and Tsvetelina Taneva, Associate, both at PETERKA & PARTNERS Bulgaria.