7 November 2017

GDPR - Guidelines on Fines to Be Imposed by Supervisory Authorities

The Article 29 Working Party (***WP29***) published its guidelines on the application and setting of administrative fines for the purposes of General Data Protection Regulation 2016/679 (***GDPR***) (the ***Guidelines***). The Guidelines provide an insight into how supervisory authorities will determine whether an administrative fine must be imposed under the GDPR.

Corrective powers of the supervisory authority

The WP29 explains that administrative sanctions provide a significant enforcement tool under the GDPR and it is important that these fines are applied in an equivalent manner throughout the EU Member States. Indeed, under the GDPR, the power to impose fines will remain with the supervisory authorities of each Member State and the supervisory authorities must observe the principles set out in the Guidelines.
Under the GDPR, supervisory authorities will have a harmonised set of corrective powers. In addition to the power to impose administrative fines, authorities can, amongst other matters:

- issue warnings or reprimands;
- impose temporary processing bans;
- order the suspension of international data flows; or
- order data controllers or processors to grant access to data subjects, correct or delete personal data.

The Guidelines indicate that supervisory authorities should determine the most appropriate corrective action for each specific situation, but should not shy away from imposing administrative fines. Accordingly, the imposition of a fine should not be regarded as a last resort in the enforcement arsenal.

Determining nature, gravity and duration of the infringement

To determine whether a fine must be imposed, the WP29 indicates that supervisory authorities will consider the nature, gravity and duration of the infringement. The GDPR establishes two categories of infringement, depending on which provisions

have been breached. These categories correspond to the (maximum) levels of fines, with a first tier of fines of up to EUR 10 million or 2% of a company's worldwide turnover, and the second tier amounting to a maximum of EUR 20 million or 4% of the worldwide turnover. An infringement qualifying for the higher level of fines would be more serious in nature. In addition, the gravity of the infringement is determined by the scope of the infringement, the purpose of the infringing processing operation and the number of data subjects affected.

On the other hand, the Guidelines explain that fines can be replaced by a reprimand if the infringement is "minor", *i.e., "it does not pose a significant risk to the rights of the data subjects concerned and does not affect the essence of the obligation in question".*

Criteria determining the choice of corrective action

The Guidelines also indicate that fines are more likely to be imposed for breaches which cause damage to the data subjects. For this purpose, "damage" should be understood as a risk for the rights and freedoms of the individual, as indicated in recital 75 of the GDPR. This recital indicates that there is such a risk:

- where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage;

- if data subjects could be deprived of their rights and freedoms or prevented from exercising control over their personal data;

- if sensitive categories of personal data are processed;

- where personal aspects are evaluated, in particular analysing or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles;

- where personal data of vulnerable natural persons, in particular of children, are processed; or

- where processing involves a large amount of personal data and affects a large number of data subjects.

Moreover, the WP29 explains that supervisory authorities will look at the possible intentional or negligent character of the infringement. For instance, on one hand, it indicates that intention can be derived from unlawful processing being authorised explicitly by top management disregarding the advice of the data protection officer.

On the other hand, failure of an employee to abide by existing policies would be indicative of negligence.

Further elements that may be considered when deciding whether a fine should be imposed, and if so, determine the amount of the fine, include:

- any action taken by the controller or processor to mitigate the damage suffered by data subjects. In particular, the WP29 indicates that the failure to take due mitigating measures could cause the supervisory authority to impose a fine instead of (or in addition to) other corrective measures;

- the degree of responsibility of the controller or processor. In other words, has the controller or processor implemented the necessary compliance measures? In order to determine what is necessary, supervisory authorities will take account of existing best practices or codes of conduct;

- any relevant previous infringements and whether corrective measures have already been imposed on the controller or processor in the past;

- the degree of cooperation with the supervisory authority;

- the categories of personal data affected by the infringement;

- the manner in which the infringement became known to the supervisory authority, for instance, whether the controller or processor notified the infringement or breach;

- adherence to approved codes of conduct or approved certification mechanisms. If such mechanisms are in place and provide for appropriate action against members who are in breach, the supervisory authority may consider that such action is sufficiently effective, proportionate or dissuasive. However, at the same time, the Guidelines state that the supervisory authority is under no obligation to take into account the sanctions pertaining to the self-regulatory authority; and

- any other aggravating or mitigating factor applicable to the circumstances of the case.

The Guidelines do not provide a detailed calculation method for determining the amount of the fine. This is likely to be set out in a potential subsequent set of guidelines.

The text of the Guidelines can be found here.

Authors

Thibaut D'hulst	tdhulst@vbb.com
Reshad Forbes	rforbes@vbb.com