WILMERHALE

The Article 29 Working Party Releases Draft Guidelines on the Application and Setting of Administrative Fines

NOVEMBER 8, 2017

One of the key components of the General Data Protection Regulation (Regulation (EU) 2016/679) ("**GDPR**") is its stronger enforcement mechanisms. Administrative fines are one of the most powerful parts of the enforcement toolbox and have raised concern among regulated organizations. On October 23, the Article 29 Working Party released draft guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679 to achieve a consistent approach by the supervisory authorities of the Member States. According to the proposed guidelines, the supervisory authority must first the identify corrective measures most appropriate for addressing the specific infringement(s). The following principles should be observed:

- **Infringement of the Regulation should lead to the imposition of "equivalent sanctions."** This concept is central in determining the extent to which the supervisory authorities are obligated to ensure consistency in their use of corrective powers, particularly in the imposition of administrative fines. Differing corrective measures chosen by the supervisory authorities in similar cases should be avoided because equivalent sanctions in all Member States are a means of preventing divergences hampering the free movement of personal data within the internal market.
- **Like all corrective measures chosen by the supervisory authorities, administrative fines should be "effective, proportionate and dissuasive."** The supervisory authority needs to impose fines that meet these criteria and, according to the Article 29 Working Party, they must apply the definition of "undertaking" as provided by the Court of Justice of the European Union ("**CJEU**") for purposes of the application of Article 101 and 102 of the Treaty on European Union and the Treaty on the Functioning of the European Union ("**TFEU**"). Here, the concept of an undertaking is understood to mean "an economic unit," which is be formed by the parent company and all involved subsidiaries.
- **The competent Supervisory Authority should make an assessment "in each individual case."** Art. 83 (4) to (6) GDPR provides a harmonized approach to breaches of obligations. Member State law may extend the application to public authorities and bodies established in that Member State and can allow for, or even mandate, the imposition of a fine for the infringement of other provisions than those stipulated in Art. 83 (4) to (6) GDPR. The Article 29 Working Party encourages the supervisory authorities to use corrective measures in a

considered and balanced approach and not to keep the fines as a last option for the enforcement of compliance with the GDPR. Further, the Article 29 Working Party announces that it will publish a binding decision on disputes between authorities, particularly regarding the determination of the existence of an infringement where the European Data Protection Board (as successor of the Article 29 Working Party) is competent to take action according to Art. 65 GDPR.

- **A harmonized approach to administrative fines in the field of data protection requires active participation and information exchange among supervisory authorities.** Supervisory authorities shall cooperate with each other and, where required, with the European Commission with the mechanisms set out in the Regulation to support formal and informal information exchanges, such as through regular workshops. To ultimately achieve greater consistency, this cooperation would focus on experience and practice in the application of the fining powers.

Second, the supervisory authorities need to consider the list of criteria laid down in Article 8 (2) GDPR when deciding whether to impose an administrative fine and determining the amount of such fine in each individual case. Therefore, the Article 29 Working Party provides for guidance on how to interpret the individual facts of the case in light of the criteria in Art. 83(2) GDPR.

- **Replacing a fine with a reprimand.** The Supervisory Authority has the option to replace a fine by a reprimand in the case of a minor infringement or where the data controller is a natural person and the fine likely to be imposed constitutes a disproportional burden.
- **Assessing the nature of the infringement.** The nature of the provisions of Art. 83 (4) to (6) GDPR is already indicated by two different maximum amounts of administrative fines. However, by assessing the facts of the case and considering the general criteria provided in article 83(2), the competent Supervisory Authority may decide that in certain cases there is a greater or a lesser need to react with the imposition of a fine as a corrective measure.
- **Assessing the gravity of the infringement.** Several different infringements committed together in any single case means that the Supervisory Authority can apply the administrative fines at an effective, proportionate, and dissuasive level with the gravest infringement as a limit. Further factors and their possible impact should be assessed:
  - **Number of data subjects.** The number of data subjects involved should be assessed to identify whether this is an isolated event or symptomatic of a more systematic breach or lack of adequate routines that are in place.
  - **Purpose of processing.** The supervisory authorities should determine the extent to which the processing upholds the two key components of this principle, namely purpose specification and compatible use.
  - **Damage suffered.** If the data subjects have suffered damages, the level of the damages to the rights and freedoms of the individual must be considered. However, the imposition of a fine is not dependent on the ability of the Supervisory Authority to establish a causal link between the breach and the material loss.
- **Assessing the duration of the infringement.** Duration of the infringement may be illustrative of, for example: (i) willful conduct on the data controller's part; (ii) failure to take

appropriate preventive measures; or (iii) an inability to put in place the required technical and organizational measures.

- **Intentional or negligent character of the infringement.** In general, “intent” includes both knowledge and willfulness in relation to the characteristics of an offence. Circumstances indicative of intentional breaches might be unlawful processing explicitly authorized by the top management hierarchy of the controller, or processing contrary to advice from the DPO. Other circumstances, such as failure to read and abide by existing policies, human error, failure to check for personal data in published information, failure to apply technical updates in a timely manner, failure to adopt policies (rather than simply failing to apply them), may be indicative of negligence.
- **Action to mitigate the damage suffered by data subjects by the infringement.** Mitigating factors are particularly suited to fine-tune the amount of a fine to the specific case. Data controllers and data processors have an obligation to implement technical and organizational measures to ensure a level of security appropriate to the risk, particularly by way of carrying out a data protection impact assessment according to Art. 35 GDPR. However, when a breach occurs, the responsible data controller or processor should do all that is possible to limit the consequences of the damage.
- **Technical and organizational measures following the principle of data protection by design or by default.** Any “best practice” procedures or methods, industry standards and codes of conduct in the respective field or profession are important considerations.
- **Previous infringements by the controller or processor.** This criterion is meant to assess the track record of the entity committing the infringement, e.g. whether the controller/processor committed the same infringement before.
- **Cooperation of the respective controller or processor with the Supervisory Authority to remedy the infringement.** The Supervisory Authority may also consider whether the intervention of the controller actually produced negative consequences to, or had a limited impact on, the rights of the individuals.,
- **Categories of personal data affected by the infringement.** The Supervisory Authority should assess whether data according to Art. 9 or Art. 10 GDPR is affected, that is, whether the data is directly available without technical protections, or whether it is encrypted.
- **Manner of the notification of the infringement.** An additional factor for setting the actual amount of a fine is whether the Supervisory Authority is made aware of the infringement through investigation, complaints, press articles, anonymous tips, or by the data controller itself.
- **Previous orders against the controller/processor regarding the same subject-matter.** The Supervisory Authority will consider prior, extensive contact with the DPO, where a controller or processor may already be on its radar for compliance monitoring following a previous infringement.
- **Approved code of conduct or approved certificate mechanism.** Where the controller or processor has adhered to an approved code of conduct, the Supervisory Authority may be satisfied that the code community in charge of administering the code takes the appropriate action, for example through the monitoring and enforcement schemes of the code of conduct, against its own members. In that case the Supervisory Authority might

decide that such measures are effective, proportionate, or dissuasive enough without the need for imposition of additional measures from the Supervisory Authority.

- **Other aggravating or mitigation factors.** Among other factors, information about profit gained by a breach may be a particularly important consideration for the supervisory authorities as economic gain from such infringement would be a strong indicator for the imposition of a fine.

Authors

Dr. Martin Braun

PARTNER

martin.braun@wilmerhale.com

+49 69 27 10 78 207