Guidelines for setting administrative fines for data infringements (2/2/18)

The expected application of the General Data Protection Regulation 2016/679 (the "Regulation") from May 2018 is likely to have some entities fretting about the huge fines. The Regulation provides for considerably higher maximum fines and describes criteria the supervisory authorities will have to consider when deciding whether to impose an administrative fine or what amount should be set. This article explores some of the criteria defined by the Regulation and a set of guidelines on the application of administrative fines drawn up by the Article 29 Working Party.[1] The criteria for applying administrative fines should be considered in both assessing an entity's data protection risks and deciding about data protection measures to be implemented.

Compared to Directive 95/46/EC, the Regulation lays a stronger foundation for setting consistent administrative fines because it is directly applicable. Under the Regulation, the supervisory authorities should ensure that applying an administrative fine is effective, proportional and dissuasive in each particular case.[2] In other words, the fine should reflect the nature and gravity of the breach and its consequences.[3]

The nature, gravity and duration of an infringement

Under article 83(2)(a) of the Regulation, deciding whether to impose an administrative fine and what amount should be set is based on the nature, gravity and duration of a breach, considering the type, scope and purpose of data processing as well as the number of data subjects affected and the extent of damage caused to them.

The Regulation provides for two different maximum amounts of an administrative fine depending on the breach:

- €10 million or 2% of annual worldwide turnover;
- €20 million or 4% of annual worldwide turnover.

Setting different maximum fines indicates that infringing some provisions of the Regulation is treated as more serious than breaching others. However, all the facts and circumstances of the case will be considered in assessing the breach, and so the amount of the fine will depend on the circumstances of the case.

The number of data subjects affected will be considered in assessing the gravity of the breach. This will allow the authorities to determine whether this is an isolated event or a more systemic non-compliance with data protection requirements.

An intentional or careless infringement

According to the working party's guidelines, an intentional breach may involve unlawful data processing authorised explicitly by the entity's management contrary to a data protection officer's recommendations (e.g. selling personal data for marketing purposes and ignoring data subjects' views about how their data should be used).

On the other hand, breaches such as failure to apply technical updates in a timely manner or failure to read and abide by existing data protection policies may indicate a careless breach.

Action to mitigate damage

Where a breach causes damage to a data subject, the data controller's or processor's actions (or inaction) to mitigate that damage will be taken into account. To mitigate the damage caused to the data subject, the data controller or processor may correct his actions or limit their impact in a timely manner by stopping a potential breach from continuing or expanding to a level with far more serious consequences.

Responsibility for implementing technical and organisational measures

According to the working party, a data controller's or processor's responsibility for implementing technical and organisational measures may include –

a) implementing technical and organisational measures according to the requirements of article 25 of the Regulation for data protection by design and data protection by default;
b) implementing appropriate data security measures; and
c) adopting and abiding by appropriate data protection policies and procedures.

Previous infringements

When a data protection breach is discovered, the entity should be examined under article 83(2)(e) of the Regulation for any breaches committed earlier. The working party explains that the supervisory authorities should assess whether the entity has committed any breaches of a similar nature or in the same way. This could be relevant where an entity has failed to properly assess its risks or respond to data subjects' requests in a timely manner, suggesting that similar breaches might be committed again as a result.

Cooperation with the supervisory authorities

Under article 83(2)(f) of the Regulation, in assessing a breach, it will be taken into account whether the entity cooperates with the supervisory authority to remedy the breach and mitigate its possible adverse effects. According to the working party, the supervisory authority will assess how the entity has responded to the supervisory authority's requests during the investigation phase to limit the impact on individuals' rights significantly as a result.

If the entity cooperates with the supervisory authority to remedy the breach and mitigate its possible adverse effects, the supervisory authority may decide to apply a lower fine. According to the working party, any cooperation that is already required by law cannot serve as the basis for setting a lower fine. So in the event of a breach it is important to carry out your statutory obligations but you should also take some extra steps to demonstrate your cooperation and help remedy the breach and mitigate its possible adverse effects.

Categories of personal data

The gravity of a breach is connected with data categories it affects. According to the working party, in

assessing what categories are affected, the supervisory authorities should consider the following factors:

- Are any of the special categories of data affected?
- Is the data directly or indirectly identifiable?
- Does the processing involve any data whose dissemination would cause immediate damage?
- Is the data directly available or encrypted?

Reporting a breach

Under article 83(2)(h) of the Regulation, the supervisory authorities will consider how they became aware of the breach, whether the data controller or processor reported it, and the extent to which it was reported.

A data controller is required by the Regulation to report a breach. Where the controller takes a careless approach, fails to report a breach, or reports only some of its circumstances, there are grounds for applying a higher fine. According to the working party, without conducting a proper assessment of the breach, the controller may be unaware of its full extent and therefore unable to provide complete information to the supervisory authority. It is important that a breach should be not only reported but also properly assessed to enable timely and complete reporting.

---

[1] This Data Protection Working Party was set up under Article 29 of Directive 95/46/EC.

[2] Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation)

[3] Guidelines on the application and setting of administrative fines for the purposes of Regulation 2016/679, which were adopted by the Article 29 Working Party on 3 October 2017