ROPES & GRAY

ALERT

London

December 21, 2017

EU data protection advisory body issues guidance on setting "effective, proportionate and dissuasive" fines under the GDPR

Attorneys
Rohan Massey

The EU's data protection advisory body, the Article 29 Data Protection Working Party (WP29), has adopted Guidelines on the application and setting of administrative fines for the purposes of the General Data Protection Regulation 2016/679/EU. Administrative fines are described in the introduction as central to enforcement and "*a powerful part of the enforcement toolbox of the DPAs*". The Guidelines are intended for use by data protection authorities (DPAs) to ensure better application and enforcement of the GDPR. They set out principles that DPAs must observe when addressing non-compliance from a controller or processor, as well as assessment criteria they should use when considering both whether a fine should be imposed and if so, the amount. Although not targeted at organisations looking to comply with the GDPR, the Guidelines provide a valuable insight into which areas organisations should focus on in order to mitigate risk arising from any breach of the GDPR.

Principles

Equivalent sanctions

Article 58(2)(b)-(j) of the GDPR sets out which tools DPAs can employ in order to address non-compliance from a controller or a processor. When using these powers, the DPAs must impose "*equivalent sanctions*". The concept of "*equivalence*" is, the Guidelines explain, "*central in determining the extent of the obligations of the DPAs to ensure consistency in their use of corrective powers*".

Effective, proportionate and dissuasive

The Guidelines explain that DPAs should employ administrative fines that are "*effective, proportionate and dissuasive*", both in national cases and in cases involving the cross-border processing of personal data.

The Guidelines recognise that national legislation may set additional requirements on enforcement procedures, which may for example include address notifications, deadlines for making representations appeals and payment. However, any such requirements should "*not hinder in practice the achievement of effectiveness, proportionality or dissuasiveness*". Precisely what this means will, the Guidelines state, be generated by emerging practice within DPAs (on data protection, as well as lessons learned from other regulatory sectors) as well as case law.

Each individual case

The Guidelines explain that the GDPR requires assessment of each case individually when deciding whether to impose an administrative fine and it is the responsibility of the competent DPA to make an assessment "*in each individual case*".

The DPA has the responsibility of choosing the most appropriate measure(s). This choice must include consideration of all corrective measures, which includes the imposition of the appropriate administrative fine.

DPAs are encouraged to use a considered and balanced approach in their use of corrective measures, in order to achieve both an effective and dissuasive, as well as a proportionate, reaction to the breach. The point, the Guidelines explain, is not to make fines a last resort, nor to shy away from issuing fines, and equally not to use them in such a way that would devalue their effectiveness.

Active participation and information exchange among DPAs

Finally, the Guidelines state that DPAs should cooperate with each other and where relevant, with the European Commission, in order to support formal and informal information exchange, such as through regular workshops.

Assessment criteria

Article 83(2) provides a list of criteria DPAs are expected to use in the assessment both of whether a fine should be imposed and, if so, the amount to be fined.

Nature, gravity and duration of the infringement

The GDPR sets two different maximum amounts that undertakings can be fined (€10 million/2% of global turnover or €20 million/4% of global turnover), which reflects the fact that that some breaches will be considered more serious than others. Supervisory authorities must assess the facts of the case in light of the general criteria provided in Article 83(2). Where it chooses to impose a fine, the tier system set out in the GDPR should be applied in order to identify the maximum fine that can be imposed.

Recital 148 of the GDPR introduces the concept of "*minor infringements*". The Guidelines explain that if the breach does not pose a significant risk to the rights of individuals, the fine may be (but does not have to be) replaced by a reprimand. Likewise, where the data controller is a natural person, and the fine would constitute a disproportionate burden, the authorities can replace the fine with a reprimand.

The Guidelines explain that the nature of the infringement, but also "*the scope, purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them*", will be indicative of the gravity of the infringement. If several different infringements are committed together the DPA can apply administrative fines "*at a level which is effective, proportionate and dissuasive within the limit of the gravest infringement*".

The number of affected individuals should also be assessed in order to identify whether the breach is an isolated event or symptomatic of a more systemic breach or lack of adequate procedures in place.

The purpose of the processing must also be assessed and the Guidelines refer to *WP29 Opinion 03/2013 on purpose limitation* (WP 203) which analysed the two main building blocks of this principle in data protection law: purpose specification and compatible use. DPAs should look at the extent to which the processing upholds these two key components.

The damage suffered by individuals should also be taken into account when determining which corrective measure to apply, the Guidelines state, although DPAs are not able to award compensation to individuals themselves. DPAs are encouraged to consider the damage suffered, or likely to be suffered, as suggested by examples of the "*risks to rights and freedoms*" in Recital 75.

It is important to note that the Guidelines state that the imposition of a fine is not, however, dependent on the ability of the DPA to establish a causal link between the breach and material loss.

The duration of the infringement should be considered. This, the Guidelines explain, may be illustrative of: (i) wilful conduct on the part of the data controller; (ii) a failure to take appropriate preventative measures; or (iii) an inability to put in place the required technical and organisational measures.

The intentional or negligent character of the infringement

The Guidelines explain that, in general, "intent" includes both knowledge and wilfulness in relation to the characteristics of an offence, whereas "unintentional" means that there was no intention to cause the infringement although the controller/processor might have breached the duty of care which is required by law.

Intentional breaches are more likely to warrant a fine. Circumstances indicative of intentional breaches might include unlawful processing authorised explicitly by top management, or in spite of advice from the data protection officer or in disregard for existing policies. Other examples include amending personal data to give a misleading (positive) impression about whether targets have been met (e.g. hospital waiting times) or the trade of personal data for marketing purposes.

Other circumstances, such as failure to read and abide by existing policies, human error, failure to check for personal data in information published, failure to apply technical updates in a timely manner, failure to adopt policies (rather than simply failure to apply them) may be indicative of negligence, the Guidelines state.

Mitigating factors

When a breach occurs and the individual has suffered damage, the responsible party should do whatever it can to reduce the consequences of the breach for the individual(s) concerned. Whether such action has been taken or not should be considered by the DPA when choosing which corrective measure(s) to apply, and in the calculation of any fine it chooses to impose.

The Guidelines explain that it can be appropriate to show some degree of flexibility to those data controllers/processors who have admitted to their infringement and taken responsibility to correct or limit the impact of their actions and should take into account the following:

1. Degree of responsibility of the controller/processor. The DPA should consider whether and to what extent the controller "*did what it could be expected to do*" given the nature, the purposes or the size of the processing. Due account should be taken of any "best practice" procedures or methods (where these exist and apply), as well as industry standards and codes of conduct.

2. Relevant previous infringements

3. Degree of cooperation with the DPA

4. The categories of the personal data affected by the infringement

5. The manner in which the infringement became known to the DPA - The Guidelines note that a controller has an obligation under the GDPR to notify the DPA about any personal data breach (notification is mandatory unless the breach is unlikely to result in a risk to the rights and freedoms of individuals). Where the controller merely fulfils this obligation, compliance should not be interpreted as a mitigating factor. Similarly, a data controller/processor who has acted carelessly without notifying the DPA, or has not notified all the details of the infringement, could be considered to merit a more serious penalty.

6. Previously ordered measures for same subject matter

7. Adherence to approved codes of conduct - The Guidelines note that adherence to an approved code of conduct can be used by the controller or processor as a way to demonstrate compliance. Such adherence might be indicative of how comprehensive the need is to intervene with an effective, proportionate, dissuasive administrative fine or other corrective measure. Further, the DPA can decide that the body in charge of administering the code can take the appropriate action itself.

8. Any other aggravating or mitigating factor – notably, the Guidelines suggest that information about profit obtained as a result of a breach may be particularly important and may constitute a strong indication that a fine should be imposed.

Comment

Little insight can be gained at this stage into the actual level of fines DPAs might apply in any given circumstances under the GDPR but it is good for organisations to know how the DPAs may be assessing and weighting elements of non-compliance in determining both whether to fine and the level of any required fine.

For organisations, whether controller or processor, the key to ensuring that any fines imposed are as small as possible is clearly compliance with **all** aspects of the GDPR. For example, if a mistake happens leading to a data security breach, it is important that policies and procedures are in place to conform with GDPR required notifications to DPAs and any subsequent follow-up or breach remediation actions. Being able to show that organisational as well as technical measures were in place to comply with obligations under the GDPR throughout the data lifecycle, will be helpful in limiting the risk and quantum of any fine imposed. Systemic failings are likely to attract higher fines so care should also be given to operational activities as failings such as the omission of a data protection impact assessment, may not come to light until a data security breach has occurred and been notified to a DPA, which means that even a low level breach could arguably trigger stiffer sanctions for accountability non-compliance at the end of any related investigation.

Data controllers and processors may take some comfort that, even with the power to issue headline-grabbing maximum fines of 4% of global of revenue under the GDPR, DPAs have been reminded by WP 29 to ensure that any fines they do impose are "*effective, proportionate and dissuasive*".

This alert should not be construed as legal advice or a legal opinion on any specific facts or circumstances. This alert is not intended to create, and receipt of it does not constitute, a lawyer-client relationship. The contents are intended for general informational purposes only, and you are urged to consult your attorney concerning any particular situation and any specific legal question you may have.