WILLIAM FRY

// PRIVACY SOURCE

The Article 29 Working Party Guidelines on the Application of and Setting of Administrative Fines for the Purposes of the GDPR

The Article 29 Working Party (now called the European Data Protection Board ("EDPB")) adopted guidelines ("Guidelines") for supervisory authorities ("SA") on the issuing of administrative fines under the General Data Protection Regulation ("GDPR").

This article provides a summary of the Guidelines.

GDPR's Enforcement Regime

The GDPR took effect on 25 May 2018. Under its enhanced enforcement regime, SA (such as the Data Protection Commission (DPC) in Ireland) are endowed with various corrective and investigatory powers (outlined in Article 58 GDPR) including the ability to issue warnings, reprimands or mandatory orders; impose bans on processing; or order the withdrawal of certification. These powers can be applied in respect of both controllers and processors of data.

Crucially, SA may also issue substantial administrative fines as well as, or instead of, the other measures listed in Article 58, with the effect that a failure to address data protection compliance obligations could prove very costly, in financial terms, for non-compliant organisations.

Under the GDPR, organisations are potentially subject to administrative fines of up to:

- €10m or 2% of total worldwide annual turnover (whichever is greater) for serious breaches; and
- €20m or 4% of total worldwide annual turnover (whichever is greater) for the most serious breaches.

The Guidelines interpret “undertaking” broadly by referring to the Court of Justice of the European Union (CJEU) case law which construes an undertaking as an economic unit, capable of encompassing several entities. The Guidelines set out that in relation to a group, this means the parent company and all involved subsidiaries in the economic unit.

Article 83 GDPR

Article 83 GDPR briefly sets out the assessment criteria for imposing and calculating an administrative fine, including the overarching requirement that a fine must be “effective, proportionate and dissuasive" in each individual case. Under Article 83, SA must also give due regard to the nature, gravity and duration of the infringement; the intentional or negligent character of the infringement; any action taken by the controller or processor to mitigate the damage; the degree of responsibility of the controller or

processor; any relevant prior infringements; the degree of cooperation with the SA and the categories of personal data affected by the infringement.

WP29 Guidelines

The Guidelines are intended for use by SA to ensure better application and enforcement of the GDPR. They are not exhaustive, nor do they purport to provide explanations about the differences between administrative, civil or criminal law systems when imposing corrective measures. Nevertheless, they build upon Article 83 GDPR, providing a deeper interpretation thereof, and its interplay with Article 58 and Article 70, under which the EDPB is empowered to specify the provisions for guidelines concerning the setting of administrative fines, and their corresponding recitals.

The Guidelines are principles-based and set out that whenever SA are using their enforcement powers, there are a number of principles which must be observed namely, that administrative fines must be "effective, proportionate and dissuasive", that the SA must make an assessment "in each individual case" that an infringement of GDPR should lead to the imposition of "equivalent sanctions" and finally, that a harmonised approach to administrative fines will require active participation and information exchange among SA.

Effective, Proportionate and Dissuasive

The Guidelines emphasise that administrative fines must adequately respond to the nature, gravity and consequences of the breach. The Guidelines set out that the assessment as to what is effective, proportionate and dissuasive in the circumstances of an individual breach will be intrinsically linked to the objective of the corrective measure chosen by the SA, i.e. whether its purpose is to re-establish compliance with GDPR, or to punish unlawful behaviour (or both). Fines are to be considered a “powerful part of the enforcement toolbox” of SA and are to be wielded in appropriate circumstances. The Guidelines advocate a Goldilocks approach such that fines are not to be imposed as a “last resort” but neither should they be used in a way which would devalue their effectiveness as a tool.

Assessment in Each Individual Case

SA must assess each case individually and choose the appropriate measure(s) carefully in order to best address the nature, gravity and consequences of the infringement. In practice this means that, once an infringement of the GDPR has been established based on a consistent and objective assessment of all the facts of a case, a SA must consider all the corrective measures available to it under Article 58 GDPR. This will necessarily involve a consideration of the imposition of an appropriate administrative fine, either accompanying a corrective measure under Article 58(2) or on its own.

Imposition of Equivalent Sanctions

The need for a consistent approach both in SA use of corrective measures, and in their application of administrative fines is stressed in the Guidelines. Breach of the GDPR should lead to the imposition of “equivalent sanctions” both in national cases and in cases involving cross-border processing of personal data. This means that, although SA remain independent in their choice of corrective measure(s), different corrective measures/different levels of fines should not be applied in similar cases. In cross-border cases consistency will be achieved primarily through the GDPR's cooperation mechanism, although the role of the consistency mechanism (which combines an advisory role for the EDPB and a role for the Commission) is also key.

Active Participation & Information Exchange

The Guidelines note that a harmonised approach to applying administrative fines requires active participation and cooperation between SA. Information should be freely exchanged, for example through regular exchanges through case handling workshops or other events which allow the comparison of cases from the sub-national, national and cross-border levels.

Assessment Claims

The bulk of the Guidelines are dedicated to delineating the various assessment criteria (both aggravating and mitigating) arising from Article 83 GDPR and providing guidance for SA on how to interpret the individual facts of a case in light of these criteria.

The Guidelines provide that the conclusions reached by SA in the first part of its assessment (i.e. in determining which measure(s) is/are appropriate) may then be used in the second part of the assessment to calculate the amount of any fine. It is clear that the particular combination of aggravating and mitigating factors in each individual case will not only tip the balance in terms of which corrective measure is to be preferred but will also, if a fine is chosen, cause the level of this fine to ratchet up or down in the SA assessment.

It is important for organisations to note that bonus points are unlikely to be awarded for an organisation's compliance with an existing legal obligation or with its obligations under the GDPR. For example, the Guidelines specifically state that controllers and processors cannot legitimise breaches by claiming a shortage of resources and, they must be able to demonstrate a risk-based approach by implementing appropriate technical and organisational measures, carrying out data protection impact assessments and mitigating risks where necessary.

The assessment criteria are as follows:

- **The gravity of the infringement**

The Guidelines provide that the nature of the infringement as well as the scope and purpose of the processing, the number of data subjects concerned, and the level of damage suffered by them will be indicative of the gravity of the infringement.

The nature of the infringement

As referred to earlier, GDPR provides for two tiers of administrative fines to reflect the fact that certain types of infringements are considered more serious in nature than others. Nonetheless, the Guidelines provide that by assessing the facts of any individual case in light of the criteria, a SA may decide that there is a greater or reduced need to react with a corrective measure in the form of a fine. Further, infringements are not given a specific quantum in the GDPR, only a maximum cap, and the Guidelines set out that breaches which might ordinarily fall into a lower category (i.e. up to 10 million euros or 2% of total annual turnover) could end up qualifying for a higher tier of fine where certain aggravating factors are present.

GDPR suggests that “minor breaches” may not necessarily result in a fine and the Guidelines agree that a SA has the option to replace a fine by a reprimand in the case of a minor infringement, e.g. one which "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" or where the data controller is a natural person and the fine likely to be imposed constitutes a disproportionate burden.

The number of data subjects

This criterion should be assessed in combination with the purpose of the processing and the damage suffered by individuals. Considering the number of individual data subjects affected may help a SA to determine whether the breach is a single isolated incident or symptomatic of a more systemic breach or lack of adequate systems in place. Of course, an isolated incident may still be very serious, depending on the circumstances of the case (as it may affect a large number of data subjects).

Purpose of the processing

The extent to which the processing upholds the "purpose limitation" principle, in regard to both purpose specification and compatible use, should be considered.

Damage suffered by individuals

Processing of personal data may generate risks for the rights and freedoms of individual data subjects and if damages have been, or are likely to be suffered, then SA should take this into account, (despite not being competent to award the specific compensation for the damage suffered themselves). Significantly, there is no need for SA to establish a causal link between the breach and the material loss in order to impose a fine.

- **The duration of the infringement**

A breach of lengthy duration is not bad per se, but it may be indicative of wilful conduct on the controller's part or a failure to take appropriate preventative measures or to put in place the required technical and organisational safeguards.

- **The intentional or negligent character of the infringement**

The Guidelines set out that "intent" includes both knowledge and wilfulness in relation to the characteristics of an offence, while "negligent" implies the breach of a duty of care. Intentional breaches are generally considered more severe than negligent ones, and therefore will be more likely to warrant the application of an administrative fine. Intentional breaches of the GDPR might be indicated by unlawful processing explicitly authorised by top management or processing contrary to advice from the data protection officer. Negligent behaviour could include failure to apply technical updates in a timely manner or failure to adopt or fully implement policies (rather than simply failure to apply them).

- **Any action taken by the controller or processor to mitigate the damage suffered by individuals**

The "responsible behaviour" (or lack of it) of an organisation in response to a breach should be considered. While organisations have an obligation to implement appropriate technical and organisational measures, if a breach occurs and an individual has suffered damage the responsible party should do whatever it can to reduce the consequences of that breach for that individual (this may include, for example, contacting other controllers/processors who may have been involved in an extension of the processing).

- **The degree of responsibility of the controller or processor taking into account technical or organisational measures implemented by them.**

SA must consider to what extent the controller "did what it could be expected to do" given the nature, the purposes, or the size of processing, in light of their obligations under GDPR. Best practice procedures or methods, industry standards and codes of conduct in its respective field or profession are important factors in this assessment.

- **Any relevant previous infringements by the controller or processor.**

The track record of the organisation and whether it has committed infringements in the past should be assessed. The Guidelines point out that a different type of breach of the GDPR may nonetheless be relevant for the assessment as it could be indicative of a general level of insufficient knowledge or disregard for the data protection rules.

- **The degree of cooperation with the SA in order to remedy the infringement and mitigate the possible adverse effects of the infringement.**

The level of cooperation by the organisation in an attempt to remedy the infringement and mitigate the possible adverse effects is deserving of "due regard". It is clear that this criteria would usually be applied when calculating the amount of a fine (rather than assessing whether or not to impose a fine in the first place) and the Guidelines specifically note that any cooperation which is already legally required should be disregarded.

- **The categories of the personal data affected by the infringement.**

SA should assess whether special categories of data are affected, whether the data is directly identifiable, whether it is encrypted, and whether the dissemination of data (which is not special category data) would nonetheless cause immediate damage/distress to the individual. The Guidelines emphasise that it should not always be considered positive that the breach only concerns indirectly identifiable or even pseudonymous/encrypted data –as an overall assessment of the other criteria in combination with these factors may still lead a SA to determine that a fine should be imposed.

- **The manner in which the infringement became known to the SA, in particular, whether, and if so, to what extent, the controller or processor notified the infringement.**

The Guidelines indicate that the manner in which the SA was made aware of the infringement will be an important consideration (i.e. did the organisation notify the SA itself about the infringement or did the SA find out through investigation, complaints, press articles or anonymous tips). In relation to personal data breaches, the Guidelines make it clear that while a proactive and responsible response to a data breach can be a mitigating factor, an organisation will need to do more than merely fulfilling its obligation under GDPR to notify the SA. The Guidelines also stress that an organisation which through carelessness does not adequately assess the extent of the infringement, and which as a result fails to notify the SA of the infringement, or does not communicate the full extent of the infringement to the SA, is likely to merit a more serious penalty.

- **Where measures referred to in Article 58 have previously been ordered against the controller or processor concerned with regard to the same subject-matter, and compliance with those measures.**

A controller or processor may already be on a SA's radar following a previous infringement, and SA should also take into account previous extensive contacts with the organisation's data protection officer.

- **Adherence to approved codes of conduct pursuant or approved certification mechanisms.**

Where the controller or processor has adhered to an approved code of conduct, the SA may decide that the community in charge of administering the code should take the appropriate action.

- **Any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement.**

According to the Guidelines, economic gain from an infringement would be a strong indication that an administrative fine should be imposed.

Conclusion

The Guidelines were adopted in October 2017 and recognise that the fining powers are a novelty for some SA and have the potential to raise issues in terms of resources, organisation and procedure. In this regard, it is important to note that the fining powers exercised by SA will be subject to appeal before national courts. Nevertheless, employing the Guidelines as a road-map, and reflecting upon the Article 83 criteria as expanded and delineated therein, should greatly assist SA in reaching coherent and consistent decisions regarding the imposition of appropriate administrative fines (in addition to or instead of other measures under Article 58) for each breach they encounter, and ultimately lead to increased certainty for organisations.

Contact Us

If you have any queries in relation to this, or would like to know more about our PrivacySource offering, please contact our Partner below, or your usual William Fry contact.

David Cullen
PARTNER
+353 1 639 5202
david.cullen@williamfry.com

Leo Moore
PARTNER
+353 1 639 5152
leo.moore@williamfry.com

John O'Connor
PARTNER
+353 1 639 51823
john.oconnor@williamfry.com

Contact our PrivacySource Team here

Follow us @WFIDEA