A&L Goodbody

WP29 Guidance on FINES

The Article 29 Working Party (**WP29**) has published Guidelines on Administrative Fines.

The guidelines emphasises the need for supervisory authorities to be consistent in their approach to fines, as discretion of supervisory authorities in regard to the application of fines may lead to divergences throughout the EU.

Background

The GDPR provides supervisory authorities with the power to impose significant fines on controllers and processors for non-compliance. Businesses will face up to €20m or in the case of an undertaking up to 4% of annual worldwide turnover of the preceding financial year, whichever is greater. Fines can be imposed in addition to, or instead of any corrective measures (such as warnings or reprimands).

Whilst some EU supervisory authorities already have the power to impose fines, such as the UK Information Commissioner who may impose fines of up to £500,000, fining powers represent a novelty for the Irish Data Protection Commissioner. Under the Data Protection Acts 1988-2003, only the Irish courts can impose fines for offences committed.

The GDPR does not impose any criminal sanctions for infringements of the GDPR, but instead defers the task of laying down rules on other penalties to Member States, who must ensure such penalties are effective, proportionate and dissuasive.

Principles

The GDPR sets out corrective powers that supervisory authorities may employ in order to address non-compliance by a controller or a processor (Article 58(2)). The WP29 states that when using these powers, the supervisory authorities must observe the following principles:

1. **Imposition of *"equivalent sanctions"***

   Supervisory authorities should apply these guidelines in the spirit of cooperation according to article 57(1)(g) and Article 63, with a view to ensuring the consistency of application and enforcement of the GDPR. Although supervisory authorities will remain independent in regard to their choice of corrective measure, the WP29 states that it should be avoided that different corrective measures are chosen by the supervisory authorities in similar cases, and the same principle applies when such corrective measures are imposed in the form of fines.

2. **Administrative fines should be *"effective, proportionate and dissuasive"***

   The assessment of what is effective, proportional and dissuasive in each case should reflect the objective pursued by the corrective measure chosen, to either re-establish compliance with the rules, or to punish unlawful behaviour, or both. When imposing fines that are effective, proportionate and dissuasive, the supervisory authority should interpret the notion of an *"undertaking"* in accordance with Articles 101 and 102 of the TFEU (Recital 150). The WP29 highlights that EU case-law interprets the concept of an "*undertaking"* as encompassing an economic unit, which may be formed by the parent company and all involved subsidiaries.

3. **Supervisory Authority must make an assessment *"in each individual case"***

   Article 83(2) sets out the factors which supervisory authorities must have regard to when deciding in each individual case whether to impose a fine and the amount of the fine.

   In regard to cross-border processing, the European Data Protection Board (EDPB) may issue a binding decision on disputes between a lead authority and concerned authorities relating to the determination of the existence of an infringement. The EDPB may also discuss how the principles of effectiveness, proportionality and deterrence are observed in the administrative fine proposed by the lead authority. Lead or concerned authorities may challenge the EDPB's decision by way of an annulment action taken before the CJEU. An annulment action may also be taken by a controller, processor or a complainant if the EDPB decision is of *"direct and individual concern"* to them (Recital 143). However, any fines imposed will be at the discretion of the lead supervisory authority (rather than the EDPB) and subject to appeal before national courts where the supervisory authority is established (Articles 78 and 83(1)).

4. **Active participation and information exchange**

   The WP29 encourages supervisory authorities to co-operate with each other and exchange information in regard to their experience and practise in imposing fines to achieve greater consistency.

Assessment criteria

A substantive part of the WP29's guidelines concerns the assessment criteria arising under Article 83(2)(a)-(k) of the GDPR, which must be considered by supervisory authorities when setting a fine. Some highlights of the WP29's commentary on the criteria are:

a. ***The nature, gravity and duration of the infringement***

The GDPR in providing for two different maximum amounts of administrative fine, €10 million or €20 million, already indicates that a breach of some provisions may be more serious than for other provisions. Breaches of the GDPR which, due to their **nature,** fall within the 'up to €10m or 2% of annual worldwide turnover' category as set out in article 83(4), may end up qualifying for the higher tier '€20m or 4% of annual worldwide turnover' category in certain circumstances. For example, where a breach has previously been addressed in an order from the supervisory authority, which the controller or processor has failed to comply with (Article 83(6)).

On the other hand, a breach may be deemed to be a minor infringement, and result in a reprimand rather than a fine being imposed, in circumstances where the supervisory authority, having assessed the criteria in article 83(2), finds that the breach does not pose a significant risk to data subjects and does not affect the essence of the obligation in question, or would constitute a disproportionate burden where the controller is a natural person.

The nature of the infringement, but also *"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. Therefore, the WP29 notes that the following factors should be assessed:

- An assessment of the **number of data subjects** involved is important in order to identify whether this is an isolated event or symptomatic of a more systematic breach or lack of adequate routines in place.
- **The purpose** of the processing should be assessed to consider the extent to which the processing upholds the principle of purpose specification and compatible use.
- If the data subjects have suffered or are likely to suffer **damage** as a result of the infringement, then the supervisory authority should consider this in its choice of corrective measure, although the authority itself cannot award compensation for the damage suffered. 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.
- The **duration** of the infringement may be illustrative of: (a) wilful conduct on the controller's part; (b) failure to take appropriate preventive measures, or (c) inability to put in place the required technical and organisational measures.

b. ***The intentional or negligent character of the infringement***

The WP29 observes that intentional breaches will more likely warrant the application of a fine than unintentional ones.

Circumstances of intentional breaches might be unlawful processing authorised explicitly by senior management, in spite of advice from the data protection officer. The WP29 gives the example of amending personal data to give a misleading impression about whether targets have been met, which we have seen in the context of targets for hospital waiting times.

Examples of negligent breaches include: failure to read and abide by existing data protection policies, human error, failure to check personal data in information published, failure to apply technical updates in a timely manner, and failure to adopt policies.

c. ***Mitigation action taken***

Supervisory authorities will take into account any mitigation measures taken when considering their choice of corrective measure(s), as well as in the calculation of the fine to be imposed.

d. ***The degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32***

The WP29 states that supervisory authorities should assess the responsibility of the controller or processor by considering:

- *Has the controller implemented technical and organisational measures that give effect to the principles of data protection by design or by default (Article 25)?*
- *Has the controller or processor implemented an appropriate level of security (Article 32)?*
- *Are the relevant data protection routines/ policies known and applied at the appropriate level of management in the organisation (Article 24)?*

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

Supervisory authorities should assess the track record of the entity committing the infringement, in particular whether it has committed the same infringement previously, or in the same manner (e.g. as a result of inappropriate risk assessment, or unjustified delay in responding to data subjects' requests).

f. ***The degree of cooperation with the supervisory authority in order to remedy the infringement and mitigate the possible adverse effects of the infringement***

The GDPR provides that the degree of cooperation may be given *"due regard"* in determining whether to impose a fine and the amount of the fine. However, it would not be appropriate to give additional regard to cooperation that is already required by law, such as allowing the supervisory authority access to premises for audits/inspections.

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

The WP29 gives examples of key questions that should be considered by the supervisory authority, including:

- *Does the infringement concern sensitive or criminal convictions' data?*
- *Is the data subject identifiable or indirectly identifiable from the data?*
- *Does the processing involve personal data whose dissemination would cause immediate damage/distress to the individual?*
- *Is the data directly available without technical protections, or is it encrypted?*

h. ***To what extent did the controller or processor notify the infringement?***

A controller has a mandatory obligation to notify the supervisory authority within 72 hours, where feasible, about personal data breaches which are likely to result in a risk to individuals' rights. The processor is only obliged to notify the controller of the breach. Where a controller or processor acts carelessly without notifying, or at least not notifying all the details of the infringement due to a failure to adequately assess the extent of the infringement, the supervisory authority may consider imposing a more serious penalty.

i. ***To what extent a controller or processor has complied with previous corrective measures imposed on them with regard to the same subject –matter***

The supervisory authority should take into account the extent of compliance with any measures they have previously issued to the same controller or processor with regard to the same subject matter.

j. ***Adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42***

Where an organisation follows a code of conduct, a supervisory authority may conclude that enforcement under the terms of the code may be sufficient without further enforcement by the authority.

k. ***Any other aggravating or mitigating factors, such as financial benefits gained or losses avoided, directly or indirectly, from the infringement***

Information about profit obtained as a result of a breach may be particularly important for supervisory authorities as economic gain from the infringement cannot be compensated through measures that do not have a pecuniary component. Therefore, the fact that a controller has profited from an infringement is a strong indication that a fine should be imposed.

Conclusion

While the GDPR gives national supervisory authorities discretion in deciding which corrective measure to impose and if a fine, the level of that fine, the guidelines stress the need for EU supervisory authorities to work together to improve consistency on an ongoing basis. The WP29 recommends the creation of a sub-group attached to the EDPB to ensure fines are applied consistently across the EU.

CONTACT US

John Whelan
Partner
+353 1 649 2234
jwhelan@algoodbody.com

John Cahir
Partner
+353 1 649 2943
jcahir@algoodbody.com

Claire Morrissey
Partner, Dublin
+353 1 649 2246
cmorrissey@algoodbody.com

Mark Rasdale
Partner
+353 1 649 2300
mrasdale@algoodbody.com

Davinia Brennan
Associate & Knowledge Lawyer
+353 1 649 2114
dbrennan@algoodbody.com