

Ireland Update: EDPB's Approach to GDPR Fines

The approach to the General Data Protection Regulation ("GDPR") fines has varied significantly across EU member states. On 16 May 2022, the European Data Protection Board ("EDPB") published draft guidelines on the calculation of administrative fines under the GDPR (the "Guidelines")¹. The Guidelines are intended to harmonise the starting point and methodology for calculating GDPR fines but not the outcome, as fines will depend on all the circumstances of the particular case.

Current Approach

GDPR fines have been trending upwards with a sharp increase in the number of headline-grabbing fines imposed on big tech in 2021 and 2022. Prior to August 2021, Google's 2020 fine of €50 million was the highest fine on record. This is now only the sixth highest recorded fine imposed for GDPR breaches². This is also reflected in the Irish Data Protection Commission's ("DPC") approach to fines, with its three largest fines being imposed in the last 12 months.

| Organisation | Fine | Date |
|------------------|--------------|----------------|
| WhatsApp Ireland | €225,000,000 | September 2021 |
| Meta | €17,000,000 | March 2022 |
| Bank of Ireland | €463,000 | April 2022 |
| Twitter | €450,000 | December 2020 |

The Guidelines introduce a harmonised five-step method for calculating administrative fines.

¹ https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-042022-calculation-administrative_en

Establishing the Number of Infringements

A supervisory authority ("SA") first identifies the processing at issue. The SA will consider whether the actions resulting in GDPR breaches result from multiple different processes, or one single process (or linked processes). Where the same or linked processes result in multiple breaches, the fine imposed will not exceed the maximum amount which applies to the most serious infringement.

Two processing operations resulting in a breach will be "linked" for the purposes of determining the fine imposed if the infringing activities forms one set of linked operations (e.g. collecting and storing data) or if the infringing activities occur in close succession. For instance, a financial institution requesting and receiving a credit check from a credit reporting agency without proper legal basis and storing this information without the appropriate safeguards, involves two infringements resulting from two processing operations: collection and storage; but because each processing operation forms part of one "linked operation," the Guidelines provide that they would be considered linked processes for the purposes of identifying the maximum fine.

Find the Starting Point Sum for the Fine Calculation

Once the relevant processing infringement(s) are identified, the SA identifies the starting point sum

² Fines imposed on Amazon (€746 million), WhatsApp Ireland (€225 million), Google Ireland (€90 million), Facebook (€60 million) and Google LLC (€60 million) now exceed this figure, with Amazon's €746 million fine being the largest to date.

("SPS") for the calculation of the fine. This will be divided into three stages:

- (a) Identifying which GDPR maximum fine category it falls into:
 - (i) 2% of the undertaking's annual turnover or €10 million (whichever is higher) for infringements falling under Article 83(4) GDPR; or
 - (ii) 4% of the undertaking's annual turnover or €20 million (whichever is higher) for infringements falling under Articles 83(5) and 83(6) GDPR.

The SA uses the higher of the two amounts to determine the GDPR maximum fine category in respect of an infringement³.

- (b) The SA then determines the overall seriousness of the infringement. This involves an assessment of the nature, gravity and duration of the infringement, the intentional or negligent character of the infringement, and the categories of personal data affected (particularly where special categories of data are affected) are taken into account (Articles 83(2)(a) ((b), and (g) GDPR respectively). The following percentages of the applicable GDPR maximum fine category will be applied depending on the level of seriousness of the infringement in order to determine the SPS:

| Level of Seriousness | Liability Cap Relative to the GDPR Maximum Fine Category |
|----------------------|--|
| Low | 0 – 10% |
| Medium | 10 – 20% |
| High | 20 – 100% |

- (c) The SA then has discretion to reduce the SPS to a lower percentage of the sum calculated in (b) as per the table below in

order to ensure the fine is effective, proportionate and dissuasive. The SA is not obliged to reduce the SPS and even if it does, it may reduce the sum only partially.

| Annual Turnover | SPS Reduced to % of the SPS |
|--------------------|-----------------------------|
| < €2 million | 0.2% |
| €2 – 10 million | 0.4% |
| €10 – 50 million | 2% |
| €50 – 100 million | 10% |
| €100 – 250 million | 20% |
| > €250 million | 50% |

Aggravating and Mitigating Circumstances

After establishing an SPS, the SA reviews aggravating and mitigating circumstances under Article 83(2) GDPR and if necessary, adjusts the fine accordingly. Factors that may be considered include:

- (a) Any action taken to mitigate the damage suffered by data subjects, with particular regard to the timeliness and effectiveness of such actions.
- (b) The degree of responsibility of the controller or processor.
- (c) Any relevant previous infringements by the controller or processor, and, in particular, whether the controller or processor has a track record of infringement.
- (d) The degree of cooperation with the SA in order to remedy the infringement and mitigate the possible adverse effects of the infringement.
- (e) The manner in which the infringement became known to the SA, in particular, whether (and if so to what extent) the

³ In order to fall within the scope of the turnover-based liability cap, the undertaking's total annual turnover of the previous financial year must amount to more than €500 million.

controller or processor notified the infringement.

There is no precise formulae for deciding the weight of each factor, and the SA has discretion as to how to adjust the SPS based on the presence of any aggravating or mitigating factors.

Checking the SPS Against the GDPR Fine Category

Once all of the above factors have been considered, the SA checks that the SPS does not exceed the threshold for the GDPR fine category under Article 83(4) – (6) GDPR. This includes consideration of whether the maximum fine is set by reference to the static thresholds of €10 or 20 million, or the dynamic threshold established by reference to an undertaking's annual turnover⁴. A turnover based maximum will only apply when an undertaking's total annual turnover of the previous year amounts to more than €500 million.

Ensuring the Fine is Effective, Dissuasive and Proportionate

Finally, the SA considers whether the fine is effective, dissuasive, and proportionate. Proportionality is reviewed by reference to the severity of the infringement and size of the undertaking. The SA may also consider unique social and economic factors, such as whether the fine would irreparably damage the business of the undertaking, as part of a proportionality assessment. The fine will be considered effective if it achieves the objectives with which it was imposed, such as to re-establish compliance with the rules, to punish unlawful behaviour, or both. The fine will be dissuasive if it produces a genuine deterrent effect on the infringing body from committing the same infringement.

⁴ Existing case law of the Court of Justice will be applied to the interpretation of "undertaking". An undertaking encompasses every entity engaged in an economic activity, regardless of its legal status or how it is financed. For example, several separate economic entities may be considered as a single "undertaking" where a parent company exercises decisive influence over the subsidiary. Determining this involves an analysis of the economic, legal

Implications for Data Controllers and Processors

The Guidelines are expected to result in a more transparent and proportionate approach to fines for small and medium-sized enterprises. The Guidelines will ensure an upward trend in fines to large organisations, particularly where a group of companies are considered as a single undertaking and the fine is calculated as a percentage of the undertaking's annual turnover. In the wake of these new Guidelines, it is clear that the days of relatively small fines for large organisations breaching GDPR is in the past. It will be interesting to see the extent to which the methodology set out in the Guidelines are applied to the calculation of any fines imposed on Instagram in the DPC's decision, which is expected to be issued this month, relating to Instagram's alleged violation of children's privacy.

Further Information

For further information, please reach out to your usual Maples Group contact or the person below.

Dublin

Claire Morrissey

Head of Data, Commercial & Technology
+353 1 619 2113
claire.morrissey@maples.com

August 2022

© MAPLES GROUP

This update is intended to provide only general information for the clients or professional contacts of the Maples Group. It does not purport to be comprehensive or to render legal advice. Published by Maples and Calder (Ireland) LLP.

and organisational links between the parent company and its subsidiary, by reference to factors such as participation, personnel or organisational ties, instructions and the existence of company contracts. Where a parent company owns all or almost all shares in an infringing subsidiary, there will be a presumption that the parent company exercised decisive influence over the subsidiary which may result in the parent company's turnover being used for the fine calculation.