Enforcement

Multi-Billion Euro Fines for Data Protection Violations Under the New GDPR—Really?

The European Union’s new privacy regime, the General Data Protection Regulation, significantly steps up the enforcement powers of the EU’s national data protection authorities by empowering them to impose fines relative to a company’s revenue, which creates many legal uncertainties, such as whether revenue from a business undertaking should be calculated relative to a single legal entity or can include a group of companies, the authors write.

BY ANDREAS GRÜNWALD, ALEX VAN DER WOLK, AND JENS HACKL

Introduction

The European Union General Data Protection Regulation (GDPR) will come into force on May 25, 2018. It will increase existing obligations for businesses, as well as introduce a number of new obligations, such as recordkeeping obligations and mandatory privacy impact assessments. But aside from the substantive obligations, the GDPR also significantly steps up the enforcement powers of the EU’s national data protection authorities (DPAs), empowering DPAs to impose fines of up to 20 million euros ($23.5 million) or 4 percent of worldwide turnover (revenue), whichever is higher.

The new sanctions framework which introduces the possibility of imposing fines relative to a company’s revenue, is unprecedented in the context of data privacy enforcement and therefore comes with legal uncertainties. Will revenue from an undertaking only relate to a single legal entity or can it also include a group of companies? What will be the relevant turnover considered for calculation of fines? When is the starting point of the calculation or the cap for maximum amounts? These concepts have until now been foreign to European privacy laws, and there is no guidance or precedent that can assist with their interpretation.

While the GDPR does not define “undertaking” it does contain a definition of a “group of undertakings” (Art. 5(19)), which means “a controlling undertaking and its controlled undertaking.” For an interpretation of the term “undertaking,” recital 150 of the GDPR refers to the principles of antitrust law (Art. 101, 102 of the Treaty on the Functioning of the European Union (TFEU)). If GDPR fines are to be determined in the same way as antitrust fines, then this may open up the fining potential under the GDPR to include the turnover of the entire corporate group to which the entity belongs, irrespective of whether the parent company itself was involved in the GDPR violation.

However, it seems worthwhile to challenge this broad understanding of the term “undertaking” and also to take a closer look at other factors in the determination of antitrust fines and how they would apply in a GDPR context.

Andreas Grünwald is a partner at Morrison & Foerster LLP in Berlin and a member of the internet, media, entertainment law practice.

Alex van der Wolk is a partner at Morrison & Foerster LLP in Brussels and a member of the firm’s privacy & data security practice.

Jens Hackl is a senior associate at Morrison Foerster LLP in Berlin.
Fines for GDPR Violations

GDPR Article 83 provides maximum fines in relation to various types of violations. There are two categories of fines, both containing a monetary maximum as well as a percentage of turnover maximum: 10 million euros ($11.75 million) or 2 percent of annual turnover, and 20 million euros ($23.5 million) or 4 percent of turnover.

The GDPR’s fining scheme will significantly increase all of the current DPAs’ fining powers, even in EU countries that already provide for relatively high fines (e.g., in Spain: 600,000 euros ($704,847), or in the U.K.: 500,000 pounds ($662,120) per violation).

How to Determine Fines Under the GDPR

With no guidance yet from either a national EU DPA or the Article 29 Working Party, the only current guidance we have is from the GDPR legislators (the European Parliament and the Council), who wanted “strong sanctions.” But aside from providing the “penalty ceiling” that may be imposed, the GDPR also provides criteria that DPAs will need to consider when “deciding on the actual amount of the fine in each individual case” (Art. 83(2)). This list includes various aggravating and mitigating factors, such as the nature, gravity, and duration of the violation, the intent or negligence of the violation, repeat offenses, and cooperation with DPAs during the investigation, as well as some privacy-specific criteria such as the categories of affected personal data and compliance with an approved code of conduct.

However, Article 83 does not provide any guidelines or factors to determine (i) the reference point for the maximum amount of the fine (i.e., the turnover of which “undertaking” should be considered), and (ii) the starting point for calculating the specific fine (i.e., which basic amount should be held against the maximum fine).

Reference Point for the Maximum Amount of the Fine—The “Undertaking” Antitrust Definition of an “Undertaking”

In a series of antitrust cases, the Court of Justice of the European Union (CJEU) established its “single economic entity” doctrine and held that the term “undertaking” should be interpreted very broadly. According to the ECJ, an undertaking “encompasses every entity engaged in an economic activity regardless of the legal status of the entity and the way in which it is financed.” This has been held to mean that companies within the same corporate group (i.e., the parent company and its subsidiaries) form one single economic entity and are thus deemed to be a single “undertaking” for antitrust purposes.

For any entity to be considered part of a corporate group, it is only required that the parent company can (de facto) exercise “decisive influence” on the behavior of that entity. According to the ECJ, there is a rebuttable presumption for the parent company to actually exercise such decisive influence where it holds all or almost all of the capital in a subsidiary (although no company has to date ever been able to rebut such presumption in practice). Otherwise, the antitrust authority would have to prove the existence of economic, organizational and/or legal links between the parent company and its subsidiary to establish a relevant corporate group. Until now, the courts have been satisfied with only minimal evidence to that end. The ECJ, for instance, confirmed the liability of both parent companies in a joint venture where one of the parent companies’ participation was less than 50 percent. The ECJ has also held that it is irrelevant whether the controlling entity is a strategic investor or has only a financial interest (which is often the case with private equity funds).

Once an entity is considered to be part of a corporate group, it is irrelevant whether the parent entity had any actual involvement in, or even knowledge about, the antitrust violation as it happened at the subsidiary level. And because the single economic entity doctrine considers the subsidiary and the parent to be one “undertaking,” the cap on any subsequent sanctions is then also calculated at the group level, i.e., taking into account the group’s turnover.

“Undertaking” Within the Meaning of the GDPR

If these antitrust principles are indeed going to apply to the GDPR, they would allow DPAs to establish a maximum penalty based on the turnover of the entire corporate group of the infringing entity. To do so, the DPA would only have to establish that the respective parent company can (de facto) exercise decisive influence on the behavior of its subsidiary. The DPA would not have to prove that such influence was specific or even actual in relation to the alleged infringing activity (but rather would have to prove influence as a general fact). This would make the burden of proof for the DPA relatively low. Moreover, where the parent holds all (or a majority) of the shares in the infringing entity, the required decisive influence would have to be assumed—again, regardless of any actual involvement.

While applying the antitrust doctrine of a “single economic entity” to the GDPR (and determining the maximum amount of GDPR fines only in relation to the turnover of the infringing entity itself) may be suggested by recital 150 of the GDPR, there are also provisions which suggest the opposite interpretation:

- First, in Article 4a, the GDPR contains a definition of a “group of undertakings” which is defined as “a controlling undertaking and its controlled undertakings.” This definition of “group of undertakings” closely resembles the notion of “single economic entity” as it is used in antitrust terms. However, Article 83 of the GDPR, when referring to the maximum fines, still only refers to the turnover of “an undertaking” and not a “group of undertakings.” This seems to suggest that the drafters of the GDPR, although familiar with the concept of “single economic activity,” still chose to explicitly not use the term “group of undertakings” in relation to fines.

- Second, corporate group liability is relatively unknown in established privacy law principles. In antitrust law, the “single economic activity” doctrine is somewhat of the flipside to the “intra-group exemption.” This means that all companies within a corporate group are allowed to enter into anti-competitive agreements (which agreements would be unlawful if they were entered into by third parties, thus the “exemption”). However, in privacy law, the concept of such an intra-group exemption is not a common notion. In fact, all requirements under the GDPR continue to apply regardless of whether personal data is transferred or processed within the corporate group. It would therefore...
be inconsistent with the provisions of the GDPR to apply the sanctions regime at a group level.

- Third, recital 150 was added into the GDPR at a rather late stage during the legislative process. The recital refers to the term “commercial undertaking,” a term with no equivalent under antitrust (case) law. The fines provision (Art. 83), however, continues to use the term “undertaking.” This suggests a certain conflict between the recitals and the body of the GDPR, which—if true—means that the provisions in the body should prevail.

Ultimately, it will be up to the CJEU to determine the full scope of the term “undertaking” under the GDPR. Until then, companies may be advised for internal risk assessment purposes to take into account that fines under the GDPR could be calculated based on the group’s turnover. It should be noted that this does not mean that every minor violation by an affiliate automatically triggers the full penalty based on the entire group’s turnover. Once it has been established that the group’s turnover can be used for the purpose of establishing the maximum penalty that can be imposed, the next step would be to determine the actual amount of the fine.

**Starting Point for the Determination of the Fine—The “Basic Amount”** As indicated above, notwithstanding the maximum penalty, the GDPR does provide for aggravating and mitigating factors in calculating the actual amount of a fine. However, it does not provide the starting point for determining the fine (to which aggravating and mitigating factors are then applied). Because Article 83 refers to the application of aggravating and mitigating factors on a case by case basis, parallels may also be seen in antitrust law.

**Attribution of Antitrust Fines**

European antitrust law permits the imposition of fines (of up to 10 percent of an undertaking’s total turnover) by the European Commission (EC). The EC, in turn, has issued guidelines, outlining how it decides a fine in accordance with antitrust law), there are also arguments against applying a framework that is similar to the antitrust laws. For example, privacy violations are not necessarily associated with the actual sale of a product or service. Where, for example, a GDPR violation relates to the processing of employee data or concerns the failure to appoint a data protection officer, there would not be any relevant associated sales to use to calculate the basic amount of the fine. As the attribution of antitrust fines is based on specific penalty guidelines issued by the antitrust regulator, it seems only warranted that for GDPR violations a similar framework of guidelines should be issued by the European Data Protection Board which is best positioned to issue such guidelines at EU level. Such guidelines could also address other specific situations, such as a violation by a subsidiary that is a fairly minor or common mistake, or a GDPR violation by a subsidiary that was also a clear violation of corporate policy.

**Conclusion and Outlook**

Because the GDPR is not yet in force, the issue of the calculation of fines is not yet critical. However, May 2018 is approaching rapidly and with 28 DPAs that are each empowered to issue fines under the GDPR, the calculation of fines will be a much more relevant topic soon. As the GDPR leaves a definitive solution for the calculation of fines unresolved, the reference to antitrust laws in the recitals creates more confusion than clarity. Absent clear guidelines on how the penalty provisions of the GDPR will be interpreted and applied by the DPAs, there is a distinct risk of varying interpretations.

While it is possible that the relevant turnover against which maximum fines may be calculated will include the annual worldwide turnover the corporate family (in accordance with antitrust law), there are also argu-
ments to support a more narrow application of the turn-over principle. By the same token, the antitrust guidelines on how to determine the basic amount of a fine do not seem to be suitable for application to the GDPR. Specific guidelines for determining the basic amount of a fine will be very necessary in the near future.

What is certain is that this topic is far from settled and is likely to be the subject of debate as the GDPR further unfolds.

By Andreas Grunwald, Alex van der Wolk, and Jens Hackl

To contact the editor responsible for this story: Donald Aplin at daplin@bna.com