# Schoenherr - A novel model for calculating GDPR fines: Companies beware!

**Competition authorities are typically lambasted for their ever-increasing fines for breaches of competition law. European Commissioner for Competition Margrethe Vestager was roasted for imposing multi-billion fines on Google. Looking at recent penalties for comparatively trivial violations of GDPR rules by some companies considerably smaller than Google, data protection authorities are not only trying to catch up, but are actually leapfrogging the antitrust enforcement in deterrence. The new method of setting GDPR fines in Germany1 will support this trend. Companies should brace themselves for a fight. They might learn from lessons in antitrust enforcement.**

It must have sent shivers through company boards in Europe when it emerged earlier this year that the Conference of German Data Protection Authorities had adopted a first of its kind GDPR fine model. If consistently enforced, it will likely lead to fines that frequently approach the maximum limit of 4 % of the implicated undertaking's (group) turnover. The announcement went hand-in-hand with a regional data protection authority making clear that it wanted to impose multimillion-euro fines for GDPR violations.
The Conference was quick to note that the model is not binding on courts or data protection authorities in other countries. However, since it is being shared with other European supervisory authorities in the context of the harmonisation procedure of the GDPR, chances are it will become the role model for other authorities as well.

**How does it work?**

In a nutshell, fines are set using a multi-step system:

→ First, daily rates derived from the company's worldwide turnover in the preceding year are calculated. This is multiplied by a factor based on the severity of the breach. The multiplier ranges between 1 to 4 for minor infringements and 12 to 14.4 for very severe infringements (the last of four levels of severity).
→ Second, the resulting amount is then adjusted depending on the degree of fault and previous breaches ("recidivism"), using a scoring system.
→ Third, adjustments are made based on aggravating and mitigating factors.
→ Finally, it is checked whether fines exceed the limit of 4 % of the respective undertaking's turnover pursuant to Art. 83 GDPR.

**First thoughts and comments: the group turnover and its questionable consequences**

A major reason for the anxiety about massive fines is the reference to group turnover as being relevant for calculating the 4 % maximum fine. The model for this rule was the concept of a single economic unit ("SEU") in antitrust law (see also Recital 150 GDPR). A company and its subsidiaries comprise a single group so that the group's total turnover is relevant for calculating fines. While broadly accepted in competition law (for Austria see for example in KOG 16 Ok 5/08 – Elevators), it is still questionable whether the same concept should be transposed into the GDPR.

For one, the positive flipside of the SEU in antitrust law is that the cartel prohibition does not apply between entities constituting an SEU. They can exchange information, agree on prices and split markets as they like. In contrast, the GDPR does not acknowledge privileged data sharing within a corporate group but imposes specific restrictions on the exchange of data between affiliated companies.

Second, the SEU concept under antitrust rules requires that the parent company can influence the commercial behaviour of the subsidiary, which is the ability to influence budgets, business plans or the appointment of key management. Commercial behaviour has no real nexus to privacy, which is at the heart of the GDPR.

Third, one of the consequences of the SEU concept will likely be that, similar to the enforcement of antitrust rules, parent companies will be liable for damages caused by subsidiaries that have violated GDPR obligations. It is doubtful whether such liability, which is based on the influence over non-privacy related behaviour, is in line with rules on guilt under tort law.

After all, it seems the main driving force behind the use of the SEU concept for fines under Art. 83 GDPR is the ability to impose more deterrent fines. Whether this takes into account the criteria required by this provision sufficiently and can properly ensure that fines are in fact proportionate is doubtful.

**Further thoughts – Defence rights under Art. 6 ECHR**

GDPR fines, like antitrust fines, must reflect the gravity and duration of the infringement as well as the circumstances of each case. The European Court of Justice has long recognised that antitrust proceedings must meet the requirements of Art. 6 ECHR (ECJ in C-185/95 P – Baustahlgewerbe; in Austria KOG 16 Ok 4/07 – Payment cards).

Despite the possibly huge fines, Art. 6 ECHR allows for sanctions by an administrative body (see for example ECtHR in 13102/04 – Impar). The key prerequisite is that there must be the possibility of appeal before a judicial body that has full jurisdiction to review the decision (see for example ECtHR in 25774/05 – Bistrovic). It is questionable whether the administrative procedures currently in place in Central and Eastern Europe comply with the requirements under Art. 6 ECHR.

As a further consequence, data protection enforcement must also offer extensive procedural safeguards, such as the right to be heard, the right to a fair trial, the concept of ne bis in idem, the presumption of innocence as well as the prohibition of retroactive effects. All these rights offer ample defence rights in the setting of fines. These defence rights also mean that the parent company must be a party to the proceedings

**Art. 83 GDPR does not allow schematic penalisation**

Finally, the Conference's approach seems too schematic to satisfy Art. 83 GDPR. It provides transparency only at first sight. Art. 83 GDPR provides a comprehensive catalogue of factors that need to be considered when imposing fines, such as the severity of the infringement and the data categories that allegedly have been misused. The Conference's approach acknowledges this by asking the "basic value" of the fine multiplier to be "aligned" to those factors. In other words, the authorities will still have to make individual assessments, and the Conference's approach fails to provide harmonisation on that end. Moreover, the schematic approach of the Conference seems to indicate that fines have to be imposed in any case. This is unsupported by national laws (in Austria Sec. 11 DPA) and by the GDPR itself, which doubtlessly give room for other sanctions, such as warnings (without fines). Bottom line: Authorities' assessments are characterised by individual considerations which should not be substituted by a too schematic approach.

## Conclusion

Companies across the region have to prepare for significant fines for GDPR violations. The best defence, as always, is to make sure that no breaches of GDPR rules occur. If, nevertheless, a breach happens and an authority launches an investigation, companies should be well aware of their defence rights. They might offer additional opportunities to bring an eventual fine down than simply relying on mitigating factors.