Level of fines for data protection infringements must be appropriate

Opinion on the European Data Protection Board's Guidelines 04/2022 for the calculation of fines under the GDPR

June 2022

Summary

According to the General Data Protection Regulation (GDPR), fines for infringements should be effective, proportionate and dissuasive in each individual case (Art. 83(1) GDPR). In this context, the determination of the amount of the fine is based on a specific assessment, which must be carried out in each individual case within the parameters provided for in the GDPR. So far, however, an inconsistent practice of data protection supervisory authorities in the assessment of fines for data protection violations can be observed within the European Union. The punishment of data protection violations can sometimes lead to disproportionate consequences for companies. Even minor violations can result in significant fines. The concept of the European Data Protection Committee (EDPB) is intended to contribute to the standardisation and transparency of the imposition of fines. Based on this, the EDPB has developed a multi-level model for setting the level of fines.

In principle, guidelines on uniform fines throughout Europe for violations of the GDPR are to be welcomed. A uniform standard helps to ensure that data protection violations result in comparable sanctions. But the concept does not sufficiently take into account the requirements of proportionality and uniformity and, at the same time, justice in individual cases. Calculating the fine according to the model presented in the guidelines can lead to disproportionate consequences for companies. Even minor violations can result in substantial fines due to the consideration of the worldwide group turnover. In the case of companies with high turnover, a data protection violation by a subsidiary could result in excessive fines that are not appropriate to the specific situation, despite a well-structured, best possible process organisation. A better predictability of possible fines for data protection violations is also hindered by the supervisory authorities' scope for assessment when classifying violations as minor, medium or severe.

Annual turnover factor is not appropriate

The link to the total turnover of a company or group of companies does not comply with the provisions of the GDPR. Only the criteria set out in Article 82 (2) of the GDPR, which do not include turnover, are decisive for the amount of a fine. According to Art. 83 (4) to (6) of the GDPR, the turnover of a company exclusively constitutes the upper limit of the fine. In addition, the direct link to the total turnover puts companies with high turnover but low profits at a disadvantage compared to industries with smaller turnover but high profits. Such unequal treatment is incomprehensible and leads to disproportionate results. It would be much more appropriate to base the treatment on the values of cartel law, which are primarily based on the financial advantage achieved by an infringement.

Direct group/corporate liability does not comply with European requirements

In its guidelines, the EDSA assumes the so-called function bearer principle. According to this, it is sufficient for the group to be fined that the violation is attributable to a part of the group. It is also not necessary that the violation was committed at the management level. This has the effect of imposing liability for data protection violations by individual group companies. In addition, according to the guidelines, there is no possibility of exculpation for the responsible company if the data protection violation to be sanctioned is attributable to an employee who behaves contrary to existing and monitored conduct instructions. This interpretation does not correspond to the European requirements. Article 83 of the GDPR neither mentions a functional company concept nor a functionary principle supposedly to be derived from it as a liability concept. Moreover, the question of the prerequisites for corporate liability in the event of violations of the GDPR is currently the subject of ongoing proceedings before the European Court of Justice (ECJ, Case C-807/21). The binding decision on how Article 83 of the GDPR is to be interpreted with regard to the liability of companies is the responsibility of the courts and not the supervisory authorities.

Impact on the working atmosphere

If even minor violations by employees can lead to substantial fines, this will cause uncertainty. The concern that even a minor mistake could result in a high fine for the employer will burden employees and jeopardise the working atmosphere. The purpose of the GDPR is to protect personal data. This goal is not supported by imposing high fines on circumstances that cannot be avoided in every case, even through exemplary organisational structures.

Contact:

BDA | DIE ARBEITGEBER
Confederation of German Employers' Associations

Labour Law and Bargaining Policy
T +49 30 2033-1211
arbeitsrecht@arbeitgeber.de

BDA is the central business association organising the social and economic policy interests of the entire German economy. We pool the interests of one million businesses with around 30,5 million employees. These businesses are associated with BDA through voluntary membership of employer associations.

Transparency Register: 7749519702-29