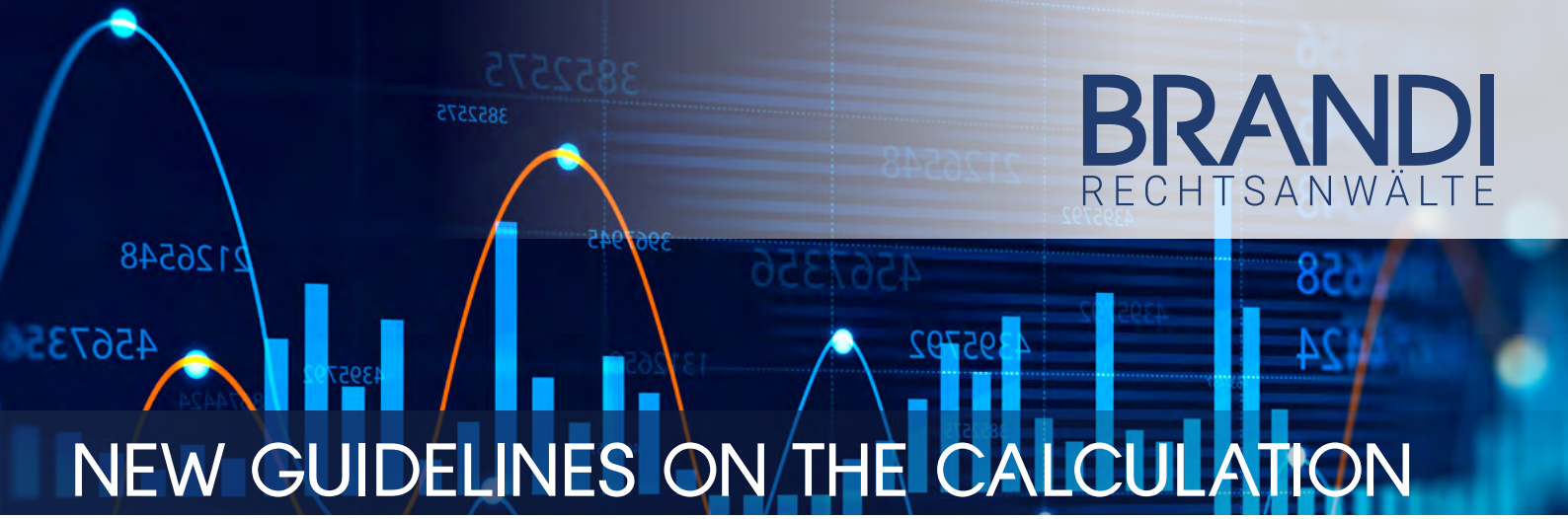

BRANDI
RECHTSANWÄLTE

NEW GUIDELINES ON THE CALCULATION OF ADMINISTRATIVE FINES

Information on data protection I September 2022

Introduction

Companies that violate data protection law may face serious consequences. The General Data Protection Regulation (GDPR) provides various options for sanctioning data protection infringements, in particular the imposition of fines in addition to the data subject's concrete claim for damages. The responsibility for fines lies with the respective data protection supervisory authorities of the federal states, in North Rhine-Westphalia, for example, with the State Commissioner for Data Protection and Freedom of Information.

Recently, numerous court decisions have increasingly focused attention on the claims for damages of those affected, but from the perspective of companies, the imposition of fines under Art. 83 GDPR poses the greater risk because, without further differentiation, there is a general threat of fines of up to EUR 10 million or up to EUR 20 million for data protection infringements.

In order to increase transparency in the calculation of fines and to ensure a uniform approach by the various supervisory authorities, the Data Protection Conference (Datenschutzkonferenz, DSK), the body of independent German federal and state data protection supervisory authorities, already published a concept for the calculation of fines in proceedings against companies in October 2019, which has so far served as the basis for calculating and setting fines against companies. The concept of the DSK is to be applied until uniform European requirements are established.

In the meanwhile, on May 12, 2022, the European Data Protection Board (EDPB), an association of representatives of national data protection authorities and the European Data Protection Supervisor, published its own guidelines on the calculation of administrative fines under the GDPR. The new guidelines are intended to harmonize the existing procedures of the individual data protection supervisory authorities of the countries and to enable more effective cooperation among the data protection supervisory authorities in cross-border cases.

The EDPB Chair Andrea Jelinek made the following comments: "From now on, DPAs across the EEA will follow the same methodology to calculate fines. This will boost further harmonization and transparency of the fining practice of DPAs. The individual circumstances of a case must always be a determining factor and DPAs have an important role in ensuring that each fine is effective, proportionate and dissuasive."

General conditions for the imposition of fines

Pursuant to Art. 83 (1) GDPR, each supervisory authority, when imposing fines, shall in principle ensure that the fine is effective, proportionate and dissuasive in each individual case. A more precise differentiation on the basis of concrete criteria is not found in the GDPR, as the intention was to create the possibility of an appropriate consideration of all circumstances of the respective individual case. Particularly in the initial phase, this resulted in a great deal of uncertainty as to how the different supervisory authorities would deal with the very broad leeway of up to EUR 20 million or 4 % of annual turnover. Potentionally subject to fines are, for example, infringements of the principles of data processing or failure to comply with the requirements for obtaining effective consent from the data subjects. It also covers the disregard of data subject's rights, such as the late provision of information, or the unauthorized transfer of data to a third country.

Art. 83 (2) GDPR only mentions individual criteria in the abstract that should be duly taken into account:

> Nature, gravity and duration of the infringement
>
> Nature, scope, and purpose of the processing
>
> Categories of personal data
>
> Number of data subjects affected and the level of damage suffered by them
>
> Intentional or negligent character of the infringement
>
> Action taken to mitigate the damage suffered by data subjects
>
> Action taken to prevent the infringement
>
> Previous infringements
>
> Degree of cooperation with the supervisory authority
>
> Aggravating or mitigating factor applicable to the circumstances of the case

The aforementioned criteria are taken up by the concepts of the DSK and the EDPB and are to be further substantiated by them.

Concept on the calculation of fines by the DSK

According to the DSK's fine concept, the points of reference for calculating the amount of the fine were the annual turnover of the com-

pany's last fiscal year, the severity of the infringement and, if applicable, the other circumstances of the individual case. The calculation of the specific fine was carried out in five steps:

1. Step: The company is assigned to a specific size class and then to a corresponding subgroup depending on the previous year's turnover.

2. Step: The average annual turnover of the respective subgroup of the size class are determined.

3. Step: The average annual turnover from step 2 is divided by 360 days, resulting in a daily rate ("basic economic value").

4. Step: The previously determined daily rate is multiplied by a factor depending on the severity of the infringement (factor 1 – 12), which is determined with reference to the graduation of fines in the GDPR (cf. Art. 83 (4) – (6) GDPR).

5. Step: The resulting calculated value is adjusted on the basis of circumstances, offender-related and otherwise, not yet taken into account.

Guidelines of the EDPB on the calculation of administrative fines

The EDPB guidelines also provide for a calculation procedure with five intermediate steps. The starting points are in particular the determination of the sactionable acts, the determination of a basic amount and the examination of aggravating or mitigating factors. Finally, it should then be verified whether the calculated amount is effective, proportionate and dissuasive within the meaning of Art. 83 GDPR.

The EDPB itself already prefaces the individual calculation steps within the framework of the guidelines with a clarification that the calculation of a fine is no mere mathematical exercise, but rather that the circumstances of the specific individual case are the fundamentally decisive factors.

The State Commissioner for Data Protection and Freedom of Information of Baden-Württemberg, Stefan Brink, has also already commented that the guidelines are not a "fine calculator". Rather, effective, proportionate and dissuasive sanctions always require a concrete consideration of the individual case.

Step 1: Identification of the processing operations and evaluation
According to the EDPB guidelines, the first step is to determine the actual conduct of the company and the legal infringement on which the fine is based. In this context, it is necessary to consider whether there are only one or several sanctionable acts and whether they result in only one or several infringements. This is required in order to determine the sanctionable infringements and the maximum amount of the fine, taking into account the regulations under competition law. In this respect, the first step is intended to take into account the requirements pursuant to Art. 83 (3) GDPR, from which it follows that, in the event of a breach of several provisions of the GDPR, the total amount of the fine may not exceed the amount for the most serious breach.

The EDPB establishes competition rules for various constellations in which one or more sanctionable conducts and, as a result, one or more infringements of legal regulations are present. The calculation of the fine depends on the number of sanctionable conduct and infringements:

> In the case when a controller violates a legal provision by only one conduct, there are no concurrences with other sanctionable conduct or legal provisions; only a fine is imposed on the basis of the one infringement.
>
> If there is more than one conduct of a controller subject to a fine, a separate fine will be calculated for each conduct. The maximum amount of the fine is determined separately for each type of conduct subject to a fine.
>
> If the conduct of a controller violates several legal provisions, a differentiation must be made for the calculation of the fine according to whether the legal provisions are mutually exclusive or apply alongside one another.
>
> If the infringement of legal provisions are mutually exclusive, for example, because one legal provision is more specific or subsidiary to another, the controller shall not be sanctioned twice for the same conduct, but the calculation of the fine shall be based exclusively on the infringement of the respective overriding legal provision.
>
> If the different legal provisions are not mutually exclusive, the fine is calculated on the basis of all infringements; the maximum fine is based on the most serious infringement.

Step 2: Determination of the basic amount for further calculation
In the second step, the basic amount for the further calculation of the fine must then be determined – similar to the DSK concept. The criteria to be applied in this respect are the provision violated by the conduct, the seriousness of the specific act, and the company's turnover.

> Violated provision: The specific conduct to be sanctioned is classified in accordance with Art. 83 (4) – (6) GDPR. The concrete classification depends on the violated provision, the interest to be protected, the significance of the regulation as well as the question to what extent the violation has prevented the effective application of the regulation and the achievement of the objective pursued by it.
>
> Seriousness of the act: The seriousness of the act is assessed on the basis of the criteria of Art. 83 (2) GDPR. The relevant factors are the nature, gravity and duration of the infringement, taking into account the nature, scope and purpose of the processing, as well as the number of data subjects affected and the damage they have suffered (Art. 83 (2) (a) GDPR), the intentional or negligent character of the infringement (Art. 83 (2) (b) GDPR) and the categories of personal data affected (Art. 83 (2) (g) GDPR).
>
> Company turnover: The company is assigned to one of six turnover groups on the basis of its total worldwide annual turnover in the last fiscal year.

Based on the provision violated and the severity of the offense, the infringement may initially be classified as low, medium or high. Depending on the categorization, a different basic value is applied for further calculation. The basic value determined in this way is then adjusted again on the basis of the company's turnover to one of the six turnover groups.

Step 3: Assessment of the other circumstances of the individual case
In the third step, the other circumstances of the specific case are to be determined and evaluated, and the basic value calculated in the second step is to be increased or decreased accordingly based on these other factors.

Among other things, the action taken by the controller to mitigate the damage (Art. 83 (2) (c) GDPR) and to prevent the infringement (Art. 83 (2) (d) GDPR), previous infringements by the controller (Article 83 (2) (e) GDPR) and the cooperation with the supervisory authorities (Art. 83 (2) (f) GDPR) must be taken into account. In addition, all other criteria arising from Art. 83 GDPR and all other circumstances relating to the specific case must of course be taken into account appropriately.

Step 4: Verification of the maximum amount of the fine
The fourth step serves to check once again whether the previously determined amount of the fine is within the legally prescribed range. In addition to Art. 83 (4) – (6) GDPR, the review must also take another look at the provisions of Art. 83 (3) GDPR (see also Step 1).

Step 5: Final overall assessment
Finally, in the fifth step, a final overall assessment of the case and the previous fine calculation must be made. In particular, it must be examined whether the amount of the fine is effective, proportionate and dissuasive in relation to the specific case.

The fine may be considered effective in accordance with the execution of the EDPB if it achieves the objectives for which it was imposed; these may be, for example, the restoration of compliance or the punishment of unlawful behavior. Proportionality exists when the amount of the fine imposed is found to be appropriate in relation to the objectives pursued, the gravity of the infringement, and the size of the company. A new adjustment may result, for example, from the social and economic context, the profitability of the company, or a loss in the value of the company triggered by the fine. Finally, a fine has a deterrent effect if it prevents individuals from violating the objectives and provisions of data protection law.

Example calculation

The calculation of a fine based on the EDPB guidelines will be illustrated by the following example:

In a hospital with an annual turnover of EUR 98 million, several employees were able to access sensitive health data that should not have been accessible to them due to their responsibilities. The hospital had implemented access restriction measures and sensitized its employees to the issue. However, due to an error in the system, employees who changed their department were still able to access the data of their original department. There was no procedure for the change of department. The problem affected about 150 out of 3500 employees. About 20,000 of the 95,000 stored data records could be accessed. In 16 instances, employees abused their remaining access rights and accessed a data set. After the incident became known, the access options of the affected employees were immediately blocked and a new process for department changers was implemented. Two years ago, there was a data protection incident at the hospital that also involved the allocation of authorizations. The further procedure was then coordinated with the supervisory authority.

Step 1

There is an infringement of Art. 32 GDPR.

Step 2

The infringement of Art. 32 GDPR falls under the infringements listed in Art. 83 (4) GDPR and thus under the less serious gradation of Art. 83 GDPR.

Accordingly, the maximum amount of the fine is EUR 10 million or 2 % of the total annual turnover achieved worldwide (in this specific case: 2 % x EUR 98 million = EUR 1.960.000). The maximum amount of the fine may therefore be EUR 10 million.

With regard to the seriousness of the act, it can be stated that the actual number of persons or data records involved, at 16, was relatively low. Nevertheless, it must be taken into account that potentially 20,000 persons or data records could have been affected under the given circumstances, and even 95,000, taking into account the systematic nature of the problem. Furthermore, negligence is to be assumed, since safety measures were taken in all other respects. Particular weight is ultimately attached to the fact that the data are particularly sensitive health data in accordance with Art. 9 GDPR.

Taking these circumstances into account, the infringement is to be classified as moderately serious, which is why the basic value for the further calculation should initially be set at 10 – 20 % of the maximum amount of the fine. Due to the fact that health data are affected, 20 % is taken as a basis. This corresponds to a preliminary basic value of EUR 2 million (20 % x EUR 10 million = EUR 2 million).

Due to its annual turnover of EUR 98 million, the hospital is to be classified in the turnover group EUR 50 million – 100 million (Group 4). For companies in this group, a value of up to 10 % of the previously determined basic value is to be applied for the further calculation. Taking into account the annual turnover, this corresponds to a final basic value of EUR 200,000 (10 % x EUR 2 million).

Step 3

Another positive aspect is that strict security measures had been taken and employees had been sensitized to the handling of personal data. Nevertheless, there was no implemented process for the specific case. Another positive aspect is the immediate adoption of countermeasures and the cooperation with the authorities. A negative aspect is the fact that a similar incident had already occurred shortly before.

Both the security measures taken previously and the cooperation with the supervisory authority are to be classified as neutral factors. Taking comprehensive countermeasures immediately should be considered a mitigating factor, while the prior data protection incident should be considered an enhancing factor. Taking all circumstances into account, the value is increased to EUR 220,000, in particular due to the previous data protection incident.

Step 4

The maximum amount of the fine was not exceeded (EUR 220,000 < EUR 10 million).

Step 5

The fine appears appropriate in the context of the final overall assessment. Accordingly, a fine of EUR 220,000 is imposed.

Conclusion

In principle, the guidelines presented by the EDPB are a step in the

right direction as far as the Europe-wide harmonization of fines is concerned. Compared to the previous calculation model of the DSK, there are also significantly more possibilities for a differentiation of circumstances, since a uniform basic value is no longer used regardless of the specific infringement.

The guidelines explicitly address various criteria of Art. 83 (2) GDPR, but also leave room for their own argumentation and elaboration in several places. However, one point of criticism remains, which has already been rightly raised against the DSK model. The size of the company alone (in terms of turnover) inevitably leads to different initial values, which accordingly already massively influence the amount of the fine at this point. This primarily concerns the categorization according to the seriousness of the infringement. While only up to 20 % of the maximum fine is imposed for low and medium infringements, the remaining fine range is only exhausted if the infringement is classified as high. However, it is positive that in the further course of the examination the profitability of the company as well as its performance and any economic advantages that the company has gained as a result of the infringement are also explicitly mentioned. So far, the German supervisory authorities have found it very difficult to include these factors and have often only allowed a threat to the existence of the company to apply in the event of a sanction.

Overall, it remains to be said that the rigid application of the guidelines by the supervisory authorities is not sufficient from the point of view of proportionality. Rather, sufficient consideration of the individual case is still required. This is also initiated by the EDPB in the context of review steps (in particular Steps 3 and 5). It remains to be seen to what extent this impetus will be used in the future. Insofar as legal action has already been taken against numerous fines in any case, we can wait in eager anticipation for the decisions of the courts of appeal.

Dr. Sebastian Meyer / Christina Prowald

Contact:

BRANDI Rechtsanwälte
Partnerschaft mbB
Adenauerplatz 1
33602 Bielefeld

Christina Prowald
Research Associate

T +49 521 96535 - 890
F +49 521 96535 - 113
M christina.prowald@brandi.net

Contact:

BRANDI Rechtsanwälte
Partnerschaft mbB
Adenauerplatz 1
33602 Bielefeld

Dr. Sebastian Meyer, LL.M.
Lawyer and Notary in and for Bielefeld
Certified Specialized Attorney in Information Technology (IT) Law
Data Protection Auditor (TÜV)

T +49 521 96535 - 812
F +49 521 96535 - 113
M sebastian.meyer@brandi.net