

# Position Paper

## EDPB Guidelines 4/22 on the calculation of administrative fines under the GDPR

### Overview

Bitkom welcomes the opportunity to comment on the European Data Protection Board's Draft Guidelines on the calculation of administrative fines under the GDPR (Guidelines 04/22). We believe that more cooperation and exchange between data protection authorities and practitioners is needed to translate the legal text of the GDPR into practice and reduce legal uncertainty.

The legal uncertainties regarding the implementation of the GDPR continue to pose problems in the market. Even with regard to the sanctions that can be imposed for violations of the GDPR, there is still no uniform application or understanding. We therefore welcome that the EDPB is trying to harmonise the approach throughout the EU.

These Guidelines complement the previously adopted Guidelines on the application and setting of administrative fines for the purpose of the GDPR, which focus on the circumstances in which to impose a fine. If the competent Data Protection Authority reaches the conclusion that a fine needs to be imposed the GDPR defines only the maximum amounts. Our goal is an EU-wide approach to implementing and enforcing the GDPR that is reasonable and free of contradictory values.

Enforcement by means of sanctions (including fines) must always be proportionate. This must also be strictly observed as a principle of administrative action.

The consideration of turnover often leads to contradiction in the case of serious offenses committed by small companies and minor offenses committed by large companies. The case-by-case nature of the sanctioning provided for in the GDPR must always be observed even if the proposed 5-step check is applied. Participation and cooperation of the affected companies have to be taken into account.

Berlin,  
27. Juni 2022

Bitkom e.V.

**Rebekka Weiß**  
Head of Trust &  
Security

T +49 30 27576-161  
[r.weiss@bitkom.org](mailto:r.weiss@bitkom.org)

Albrechtstraße 10  
10117 Berlin

Präsident  
Achim Berg

Hauptgeschäftsführer  
Dr. Bernhard Rohleder

## Bitkom Assessment

The EDPB's Guidelines contradict the GDPR in some respects and still leave too much room for different interpretation of the administering of fines.

The focus on turnover contradicts the regulations and values of the GDPR, which uses the turnover of the affected company as the upper limit, but not as the lower limit of the sanction.

Bitkom has also commented in detail to the previous Guidelines published by the German DSK regarding administrative fines. Our previous Position Paper can be downloaded on the Bitkom website.<sup>1</sup> We welcome that some of our comments and criticism are reflected in the EDPB's version of the concept.

The aim of this position paper is to draw attention to some details of the Guidelines that in our view do not sufficiently reflect the GDPR's rules and intentions regarding the imposition of fines. We would welcome discussion of these aspects and always welcome the opportunity to in-depth discussion on the subject.

## Details

While we generally welcome the EDPB's Guidelines and their aim to harmonise the considerations and imposition of fines throughout the EU, some aspects need more consideration and, in our view, adjustment as well.

Generally, the Guidelines would greatly benefit from **more real-life, practical examples** to give more guidance. We also urge the EDPB to reconsider all paragraphs that refer or concern national administrative procedures and rules which cannot be modified or otherwise impacted by the GDPR.

Another important aspect is the impact of **Codes of Conduct (CoC)**, adherence to such Codes and the mitigating effect of such adherence with regard to sanctions. Bitkom has always welcomed the strengthening of CoCs that came with the GDPR and is part of several groups and projects to develop such Codes. It is the stated intent of the GDPR that adherence to an approved CoC provides not only more legal certainty but also a mitigating factor when sanctions are imposed. The significance and meaning of Art. 82 para 2 is not sufficiently taken into account in the Guidelines.

<sup>1</sup> [https://www.bitkom.org/sites/main/files/2019-12/20191216\\_bitkom-kommentierung-bussgeldkonzept-der-dsk-finalone-pager.pdf](https://www.bitkom.org/sites/main/files/2019-12/20191216_bitkom-kommentierung-bussgeldkonzept-der-dsk-finalone-pager.pdf)

As we already elaborated in detail in our previous position regarding the “Bußgeldkonzept der DSK” (The German DPAs Guidelines), Art. 83 refers to the total worldwide annual turnover only with regard to the assessment of the **maximum amount of the fine**. As in antitrust law, the relevant geographic and product market in which the infringement took place should also play a role in the prior assessment of the fine. Otherwise, if the infringement is limited to only part of the data processing or is due to the failure of an employee, unreasonably high fines would be imposed.

Another important aspect should be included and considered in the re-draft of the Guidelines: In accordance with **international accounting standards** (especially IFRS 17) and to ensure comparability with other sectors, when determining the turnover of insurance companies, amounts the insurer is obligated to repay the policyholder regardless of whether the insured event occurs (so-called investment component) should be excluded.

Furthermore, the following **details and paragraphs** should be amended/corrected:

Regarding paras 5, 7: Fine calculations should be meaningfully transparent. If the actual fines imposed by supervisory authorities are to be effective and dissuasive it is important that controllers and processors understand the factors that contributed to particular decisions and it is essential for supervisory authorities to provide a meaningful level of transparency in this regard. The Guidelines should make this clearer.

Para 18 states: *“In certain circumstances the supervisory authority may consider that certain infringements can be punished with a fine of a predetermined, fixed amount. It is at the discretion of the supervisory authority to establish which types of infringements qualify as such, based on their nature, gravity and duration. The supervisory authority cannot make such a determination if this is prohibited or would otherwise conflict with the national law of the Member State.”*

In our view, this is not comprehensible as it cannot be derived from the GDPR. One of the most important tasks of the EDPB is to ensure uniform application.

Regarding para 33, 35 (and also 83): Proposed guidance on concurrent infringements requires further clarification to avoid unlawful double sanctioning of an offender for the same wrongdoing. Supervisory authorities need to consider legal principles on concurrence - this should be clarified.

Para 47 states: *“The EDPB considers that the calculation of administrative fines should commence from a harmonised starting Point. This starting point forms the beginning for further calculation, in which all circumstances of the case are taken into account and weighted, resulting in the final amount of the fine to be imposed upon the controller or processor.”*

In our view, the approach of calculating a starting point based on the severity of the breach as well as the turnover is not comprehensible and not in line with the GDPR.

Para 48 includes references to a “minimum fine”. In our view, this should be clarified as the GDPR does not know a "minimum fine".

Para 52 et seq state: *“Additionally, the GDPR provides that due regard should be given to circumstances that qualify the seriousness of the infringement in an individual case. More specifically, the GDPR requires the supervisory authority to give due regard to the nature, gravity and duration of the infringement, taking into account the nature, scope or purpose of the processing concerned, as well as the number of data subjects affected and the level of damage suffered by them (Article 83(2)(a) GDPR); the intentional or negligent character of the infringement (Article 83(2)(b) GDPR); and the categories of personal data affected by the infringement (Article 83(2)(g) GDPR).”*

In our view, this derives from the GDPR as the assessment of "seriousness" on the basis of individual aspects from Art. 83 (2) GDPR is not comprehensible.

Para 54 lit. b) and Art. 83 para 2 lit a) derive from the GDPR and should therefore be amended. The GDPR does not include a concept of "potentially affected". The present interpretation is therefore too broad.

Para 54 lit. b) too is too broad: The term and concept of "likely to have been suffered" is an excessive interpretation of the wording of Art. 83 (2) (a) GDPR.

Regarding para 54c: Fining methodologies should not take conduct pre-dating the GDPR into account as this would be unlawful and outside the powers of supervisory authorities.

In Para 57 it should be clarified that no fine can be imposed at all without negligence.

Para 61 describes three levels of seriousness. We don't see where the 3 levels (low/medium/high) derive from and such a concept seems to be too narrow to account for the variety of infringements.

Regarding Para. 66/67 it is in our view not clear why the EDPB use a classification "only" into these groups of company sizes. While we understand that the EDPB's intention was to account for the needs of smaller companies it is not entirely clear whether this application always leads to a “fair” consideration.

Regarding para 77: Mitigation actions undertaken after DPA investigations begin should still have mitigating value on fine levels. The risks described in para 77 are overly restrictive and the paragraph is overly prescriptive when it distinguishes between actions taken before and after the start of an investigation. It would be more helpful to refer to timeliness of actions once the controller or processor is aware of the infringement.

Para 111: This point should be further specified (e.g., through more and concrete examples). A description of the specific circumstances would lead to more harmonization, e.g., in the sense of a requirement that can be applied.

In para 118 et seq. the antitrust law concept of an enterprise/ the functional concept of an enterprise is referenced, which can lead to the consideration of e.g. the group turnover. It is not undisputed whether this reference is really what the GDPR intended.. Neither do data protection violations of data protection law regularly have the effect of increasing sales, nor are they always based on the intention of improving profits. Considerable economic damage, as in the case of large corporate cartels or abuse of a monopoly-like market position are to be expected in the case of violations of data protection obligations. In this respect, as is also the case with Art. 83 (2) sentence 2 k) of the GDPR, the concrete financial gain from the infringement is the appropriate economic criterion in data protection law for the assessment of the amount of the fine. The link to the total annual turnover of a company is in our view irrelevant/extraneous. The Guideline, in general, over-emphasizes the importance of the size and turnover of organizations when calculating fine levels. Worldwide turnover of the wider undertaking is not the appropriate starting point. Applying total turnover of the undertaking at the outset would, be legally incorrect, as it would produce a disproportionate and excessive fine; an approach recognised by the Commission in the competition law model on which the GDPR is based.

Para 120: It is disproportionate to use group sales as a basis. Using such a criterion would mean that minor violations will result in extremely high fines.

Para. 123 should be amended as it leads to a direct corporate liability, which then is established independently of whether a management body has also committed an infringement. This is the case that the KG Berlin has submitted to the ECJ, because LG Berlin and LG Bonn have ruled differently on the applicability of §30 OWiG.

Para 138 of the guidelines should also be reconsidered as there are specific circumstances not yet reflected in full: the turnover within the meaning of Art. 83 GDPR is to be understood in terms of the net turnover of Directive 2013/34/EU on the annual financial statements, consolidated financial statements and related reports of certain types of undertakings (Annexes V or VI to Art. 13 (1) of Directive 2013/34/EU). For insurance companies, insurance premiums shall be included in the revenue (page 36 footnote 62).

Publicly traded companies, which are obliged to prepare consolidated financial statements, are required to do so in accordance with international accounting standards (IFRS). In this context, it is especially important with regard to insurance companies that the International Accounting Standards Board (IASB) issued a new accounting standard “IFRS 17 Insurance Contracts” in May 2017. The IASB published amendments to the standard in June 2020 (with IFRS 17 the standard was incorporated into European law). The regulation determines that all publicly traded insurance companies shall apply IFRS 17 for their consolidated financial statements at the latest as from the commencement date of its first financial year starting on or

after 1 January 2023. IFRS 17 states that the information on the insurance revenue (first line of the profit and loss statement) shall not include amounts the insurer is obligated to repay the policyholder regardless of whether the insured event occurs (so-called investment component). These amounts that represent the investment of the policyholder (e.g. the savings component of an endowment life insurance) have to be excluded from the revenues in the profit and loss account.

Through this explicit requirement, the IASB in its role as a global standard setter in the field of international accounting has ensured the comparability of financial reporting by insurers and companies from other sectors. The investment component is comparable to the customer's investment at banks. Furthermore, for the purposes of the insurers' internal accounting vis-à-vis the financial supervisory authorities all insurers (regardless of whether they apply IFRS 17) have to present these amounts separately in order to enable their easy identification for each fiscal year.

To ensure the comparability of insurance companies with other sectors and to ascertain equal treatment with other sectors when calculating administrative fines under the GDPR, regardless of the applied regulatory framework for their accounting (IFRS 17 or national provisions based on the EU-Accounting Directive/Insurance Accounts Directive) amounts that the policyholders are entitled to should not be used to determine the starting point for the calculation of fines.

For the purpose of determining the revenue of insurance companies, footnote 62 of the EDPB draft guidelines 04/2022 currently seems to exclusively focus on the paid insurance premiums. It is therefore imperative to complement the footnote. This would prevent contradictions with the explicit requirements of IFRS 17 and guarantee proportionate treatment of insurance companies that draw up their accounts in accordance with the Insurance Accounts Directive. In conclusion, equal treatment of companies across different sectors would be accomplished.

Bitkom vertritt mehr als 2.700 Unternehmen der digitalen Wirtschaft, davon gut 2.000 Direktmitglieder. Sie erzielen allein mit IT- und Telekommunikationsleistungen jährlich Umsätze von 190 Milliarden Euro, darunter Exporte in Höhe von 50 Milliarden Euro. Die Bitkom-Mitglieder beschäftigen in Deutschland mehr als 2 Millionen Mitarbeiterinnen und Mitarbeiter. Zu den Mitgliedern zählen mehr als 1.000 Mittelständler, über 500 Startups und nahezu alle Global Player. Sie bieten Software, IT-Services, Telekommunikations- oder Internetdienste an, stellen Geräte und Bauteile her, sind im Bereich der digitalen Medien tätig oder in anderer Weise Teil der digitalen Wirtschaft. 80 Prozent der Unternehmen haben ihren Hauptsitz in Deutschland, jeweils 8 Prozent kommen aus Europa und den USA, 4 Prozent aus anderen Regionen. Bitkom fördert und treibt die digitale Transformation der deutschen Wirtschaft und setzt sich für eine breite gesellschaftliche Teilhabe an den digitalen Entwicklungen ein. Ziel ist es, Deutschland zu einem weltweit führenden Digitalstandort zu machen.