

Draft Guidelines 04/2022 on the calculation of administrative fines under the GDPR

Consultation of the EDPB

AFEP contribution

The European Data Protection Board (EDPB) adopted mid-May draft [guidelines](#) on how to calculate the amount of administrative fines that European Data Protection Authorities can impose under the General Data Protection Regulation (GDPR). This draft is subject to consultation until 27 June 2022.

To help national authorities calculate these fines, this draft intends to establish harmonised starting points by taking into account three elements: the categorisation of infringements by nature, the seriousness of the infringement and the turnover of the company. A five-step method is then proposed.

AFEP member companies have carefully analysed this draft. It calls for general and specific comments.

- **General comments**

Businesses thank the EDPB for these draft guidelines. Indeed, they appreciate documents that are likely to provide them with a better understanding of their obligations as well as better consistency in the approach of national supervisory authorities.

This framework is all the more interesting as any daily operation on data induced by the smooth running of a company might generate one or more breaches of the GDPR (research, marketing, customer relations, support activities and others).

While they consider with interest this methodological proposal focusing on fines that may be imposed by national supervisory authorities, companies nevertheless stress that fines are not the only tool at their disposal. Each of them has the power to adopt various corrective measures, the scope of which is often very efficient. (See, for example, the decision of the Belgian personal data protection authority ordering the Interactive Advertising Bureau Europe -IAB-, an organisation representing stakeholders in Internet advertising, to submit an action plan within a specific timeframe in order to remedy the shortcomings observed in the Transparency and Consent Framework -TCF, a tool used to record the consent of Internet users)

Furthermore, it seems important that the EDPB draft guidelines are in line with the regulatory framework imposed by the GDPR without introducing provisions that over-interpret the European regulation, either in the calculation of the amount of the fine or in the inclusion of the processor in the calculation methods.

AFEP thus considers that the policy of fines imposed by national authorities must be balanced against the vast toolbox at their disposal. It proposes that the latter be mentioned in the introduction to the EDPB guidelines as a means available to the authorities in their enforcement action of which fines are only one element.

Furthermore, businesses encourage the EDPB to fully comply with the RGPD in the envisaged calculation methods.

- **Specific comments**

Beyond the complexity of the proposed system (see in particular Chapter 3), the analysis of the various chapters devoted to the methodology for calculating fines gives rise to various comments or questions as to their pragmatism (a), the proportionality of the fines envisaged (b) and the consideration given to mitigating circumstances in their calculation (c).

a) Pragmatism of the envisaged guidelines

- *Towards greater consistency in the calculation of fines by national authorities*

The diverging practices of supervisory authorities in the imposition of fines legitimise the EDPB approach.

Indeed, in 2020, only five out of 27 national authorities imposed fines with an annual total of more than EUR 1 million. Only 2% of the fines imposed by all these authorities were above €500,000.

While the objective of harmonising these approaches appears necessary, the draft guidelines, which are in line with the principle of independence of data protection authorities, leave a lot of room for manoeuvre to these authorities. In this respect, the EDPB underlines that the draft guidelines intend to offer a calculation methodology rather than a harmonisation of the outcome (§5).

The objectives of harmonisation and coherence desired by the economic actors are not very pragmatic since :

- § 18 leaves it to the discretion of the national authorities to determine the types of infringements that may be penalised by a fine or a predetermined fixed amount,
- § 48 provides that the existence of a starting point for the calculation of the fine does not prevent the national authorities from lowering or increasing the fine if the circumstances of the case so require, while, at the same time, the provisions allowing the amount to be reduced are not very developed (Chapter 5).

The consequence is to (re)create a distortion between Member States as :

- some headquarters fall under the supervision of authorities that are stricter in their control policy;
- non-European players choose to locate their headquarters in Member States where these authorities have a reputation for being particularly lenient.

It is proposed to move towards a better balance between the necessary respect of the principle of independence of data protection authorities and a methodological objective which should, according to companies, tend towards more pragmatism.

In this respect, the EDPB could advocate for more consistency in the imposition of fines in order to limit competitive distortions between different data protection authorities.

- *Complementing the illustrations provided to highlight breaches by controllers with examples of breaches by processors*

Chapter 3 is devoted to concurrent infringements and the application of Article 83(3) of the GDPR. This states that “if a controller or processor intentionally or negligently, for the same or linked processing operations, infringed several provisions of GDPR, the total amount of the administrative fine shall not exceed the amount specified for the gravest infringement.” (§ 40)

At the same time, many paragraphs of the draft Guidelines underline the fact that, for example:

- the controller or processor does not need to have too much information to calculate the possible amount of the fine (§5)
- the fine imposed on a controller or processor ranges from a minimum to the legal maximum (§ 48),
- the controller or processor may take measures to mitigate the damage suffered by the data subjects (§ 74 et seq.).

By underlining the constraints or obligations on the controller or processor, the EDPB is fully in line with the GDPR.

However, at the same time, the numerous illustrations provided in Chapters 3 and 4 are primarily aimed at controllers, suggesting that processors are not (or hardly) subject to fines -as opposed to the controller.

However, for example :

- in its recent deliberation of 15 April 2022 , the French CNIL imposed an autonomous sanction on a processor for breaches of its data security obligations;
- a decision of the Polish authority in January 2022 sanctioned the controller as well as the processor for failure to ensure data security.

In the light of these references, companies propose to enrich the illustrations provided by the EDPB with examples of failures on the part of both the controller and the processor.

b) Proportionality of the fines envisaged

The undertakings take note of the fact that the EDPB draft :

- takes into account in Chapter IV three elements forming the starting points for calculating the amount of the fine: the category of infringement, its seriousness and its nature, gravity and duration;
- emphasises the need to take account of all the circumstances of the case in assessing the gravity of the infringement (§ 52 to 55 of the Guidelines).

These various references contribute to the principle of proportionality required in any sanctioning process.

However, companies have questions regarding various provisions that could jeopardise the search for proportionality of the fine. They concern in particular :

- *the gravity of the infringement (§ 54)*

In this case, point b) specifies that the assessment of this criterion is based on specific circumstances and cases, in accordance with Article 83(2) of the GDPR.

Point b- iii) deals with the purpose of the processing and states that it will lead the supervisory authority to give more weight to this factor.

In this context, businesses question the exact scope of the following sentence which states that "the supervisory authority may also consider whether the purpose falls within the so-called core activities of the controller."

The purpose of a processing operation may be intrusive without being the core activity of the company concerned (controller or processor).

This could be the case, for example, of a logistics company (without any Internet activity) which implements a facial recognition system to control the access of its employees to confidential areas of its warehouses.

In view of this example, it would be desirable for the guidelines to clarify what is meant by "core business".

- *the intentional or negligent character of the breach (§ 56 and 57)*

Apart from the fact that, once again, example 4 provided in § 56 only refers to the controller (see comments above), companies consider that the EDPB draft should explicitly recall the framework of the GDPR.

As the latter is based on a risk-based approach, these same authorities must have the possibility to take into account risk assessments made in good faith by companies without these being considered voluntary and intentional violations of the GDPR.

Efforts to protect data and reduce the risk of harm to individuals that are put in place by companies should be able to be taken into account to reduce the basis for calculating the amount of the fine, although at this stage the draft does not say so.

- *the role given to the opinions of the DPO*

Companies question the role given to the advice of the Data Protection Officers (DPO) in the examples provided in § 56 (example 4) and § 63 (example 5a).

The failure to take into account the advice of the DPO is systematically retained in the examples given by the EDPB.

This puts considerable pressure on the advisory role of DPOs, which may lead to almost systematic fines. In view of this approach, it is necessary to recall that, as part of their tasks (Article 39.2 of the RGPD), DPOs must focus their attention on the risk associated with the operations presented to them.

The organisation of compliance with the RGPD in companies -as data controller or processor- can thus pragmatically lead them not to automatically solicit the DPO on all types of subjects.

Companies suggest that the EDPB recall in the examples put forward that requests to the DPO are not systematic and depend on the policy adopted within the companies.

- *the company's turnover with a view to imposing an effective, dissuasive and a proportionate fine (4.3)*

In the comments to § 65, the EDPB considers that "it is fair to reflect a distinction of the size of the undertaking [...] and therefore takes into account its turnover".

While the provisions of Article 83 of the GDPR establish amounts and percentages in relation to the nature of the breach, its seriousness and its impact on the individual, they do not include the size of the undertaking as one of the many elements for deciding the amount of the administrative fine.

Furthermore, the approach of taking into account the size of a company's turnover to contribute to imposing an effective, dissuasive and proportionate fine calls for the following comments:

- The GDPR aims to protect the processing of personal data as such,
- A security breach in a small company (in terms of turnover) can have a considerable impact on the protection of personal data of a potentially large number of people,
- Conversely, a breach of security in a large company that manages pseudonymised data for commercial purposes may have no consequences for the individuals concerned,
- Finally, a breach of the GDPR does not necessarily impact a company's turnover, unlike - for example - an anti-competitive practice where the amount of the fine takes into account the value of the sales affected by the practice.

Moreover, only data used for commercial purposes can directly or indirectly generate a turnover. Conversely, for the processing of employee data, for example, this method of calculation does not seem to be relevant if no turnover is generated.

It is regrettable that this criterion, whose correlation with the infringement is hardly demonstrated if not for its "correctness", has such radical consequences for the calculation of the starting amount as outlined in § 66 and 67.

The envisaged methodology distinguishing the size of the undertaking based on its turnover - and not the size of the infringement - as one of the elements for calculating the amount of the fine does not, therefore, seem appropriate or even proportionate.

c) *A modest consideration of mitigating circumstances*

Chapter 5 deals with aggravating or mitigating circumstances to be taken into account.

Article 83 (2) of the GDPR states that "when deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case [...]: any action taken by the controller or processor to mitigate the damage suffered by data subjects."

- The EDPB draft seems to be a step back from this provision

Paragraph 76 of the draft guidelines mentions that "The adoption of appropriate measures to mitigate the damage suffered by the data subjects may be considered a mitigating factor, decreasing the amount of the fine."

Companies regret that the actions taken to mitigate the damage suffered by the data subject are not more taken into account by the EDPB, whereas :

- the principle of accountability leads economic actors to proceed as soon as possible to repair this breach or even to notify it to the supervisory authorities when the security breach is likely to create a risk to the rights and freedoms of natural persons,
- In certain situations, data controllers and processors must strike the right balance between the fundamental right to data protection and other fundamental rights (e.g. freedom of thought, conscience and religion, freedom of expression and information).

Supervisory authorities should be able to take into account the complexity for undertakings to balance these different rights appropriately by considering the need to respect other fundamental rights as a mitigating factor in the calculation of a fine.

- *Take better account of codes of conduct.*

Companies believe that § 104 should more explicitly emphasise that compliance with a code of conduct and the absence of a sanction by the code's supervisory body should constitute an attenuating circumstance in the calculation of a fine.

As with many good corporate governance compliance programmes, adherence to and consistent compliance with a code of conduct that may go beyond the standard obligations of the GDPR requires substantial investment by companies, which should be rewarded for doing so.

*

ABOUT AFEP

Since 1982, AFEP brings together large companies operating in France. The Association, based in Paris and Brussels, aims to foster a business-friendly environment and to present the company members' vision to French public authorities, European institutions and international organisations. Restoring business competitiveness to achieve growth and sustainable employment in Europe and tackle the challenges of globalisation is AFEP's core priority. AFEP has over 110 members. More than 8 million people are employed by AFEP companies and their annual combined turnover amounts to €2,600 billion. AFEP is involved in drafting cross-sectoral legislation, at French and European level, in the following areas: economy, taxation, company law and corporate governance, corporate finance and financial markets, competition, intellectual property and consumer affairs, labour law and social protection, environment and energy, corporate social responsibility and trade.

Contact:

Emmanuelle Flament-Mascaret, Director of Economic Law / concurrence@afep.com
Alix Fontaine, EU Policy Advisor / a.fontaine@afep.com