Centre for Information Policy Leadership
HUNTON ANDREWS KURTH

24 June 2022

# CIPL Response to the EDPB Guidelines 04/2022 on the calculation of administrative fines under the GDPR

The Centre for Information Policy Leadership (CIPL)[1] welcomes the opportunity to comment on the European Data Protection Board (EDPB) draft Guidelines 4/2022 on the calculation of administrative fines under the GDPR.

CIPL supports the EDPB's commitment to creating a more harmonised enforcement approach based on a common understanding and consistent application of the GDPR. An effective and proportionate regulatory response—which reflects a modern, strategic approach to regulatory engagement that achieves better outcomes for individuals, society and regulated organisations while maximising the regulator's effectiveness—is crucial for the proper functioning of the GDPR.

CIPL commends the level of effort and research that has gone into these Guidelines. Much of it consists of helpful explanations and insights into the EDPB's understanding of certain concepts.

However, CIPL has identified certain shortcomings, misperceptions, and ambiguities that need to be addressed before the adoption of a final version**,** mainly relating to the following six points of the Guidelines:

- An overly mechanical approach to calculating fines;
- Worldwide turnover is not an appropriate starting point for calculating a fine;
- Ambiguities related to concurrent infringements, unity of conduct and multiple infringements;
- Misperception concerning the concept of corporate liability in the GDPR;
- The overall accessibility of the Guidelines;
- Lack of accountability as a mitigating factor in regulatory enforcement.

We provide more detailed comments on each of these points below.

[1] CIPL is a global privacy and data policy think and do tank in the law firm of Hunton Andrews Kurth LLP and is financially supported by the law firm and 90 member companies that are leaders in key sectors of the global economy. CIPL's mission is to engage in thought leadership and develop best practices that ensure both effective privacy protections and the responsible use of personal information in the modern information age. CIPL's work facilitates constructive engagement between business leaders, privacy and security professionals, regulators and policymakers around the world. For more information, please see CIPL's website at http://www.informationpolicycentre.com/. Nothing in this submission should be construed as representing the views of any individual CIPL member company or of the law firm of Hunton Andrews Kurth.

**CIPL recommendations**
The EDPB should consider:

- Removing worldwide turnover as a starting point for calculating a fine.
- Avoid over-applicating competition law concepts that do not have a basis in the context of the GDPR.
- Develop a common approach to take member state statutes of limitations on prior infringements into account.
- Consider using the time of awareness of an infringement, not the beginning of an investigation as the timeframe for considering actions taken to limit the damage to the individual rights as a mitigating factor.
- Avoid duplicating the sanction already imposed by a monitoring body that monitors compliance with a code of conduct. The fact that a data controller was already sanctioned should be part of the consideration when imposing a fine to avoid disincentivising the use of codes of conduct.
- Further clarifying parts of the Guidelines. The Guidelines should be easy to understand by data protection authorities but also controllers and processors irrespective of sophistication level.
- Including compliance with internal accountability, data protection management programs, codes of conduct or any other external certification program as a mitigating factor when calculating the fine.

## I. A mechanical approach to imposing fines fails to address the protection of individuals' fundamental rights

The research underpinning the Guidelines appears to focus heavily on EU competition law. We agree that it can be helpful to look at other areas of law to assess and interpret provisions of the GDPR. For example, Recital 150 GDPR references Articles 101 and 102 Treaty on the Functioning of the European Union ("TFEU") to understand the term "undertaking" (and this interpretation is not repeated in the actual text of the GDPR).

However, it is essential to remember the nature and genesis of data protection law in the European Union and its Member States. The legal basis of the GDPR, in particular, is Article 16 TFEU,[2] and data protection is rooted in human rights, and Articles 7 and 8 of the Charter of Fundamental Rights of the European Union (hereinafter referred to as "the Charter") form the foundation of data protection

[2] Case C-645/19, *Facebook Ireland Ltd and Others v Gegevensbeschermingsautoriteit*, paragraph 44 states: "Unlike Directive 95/46, which had been adopted on the basis of Article 100 A of the EC Treaty, concerning the harmonisation of the common market, the legal basis of Regulation 2016/679 is Article 16 TFEU".

rights. The individual is at the heart of those rights. Data protection is not purely a commercial or consumer law but an expression of fundamental human rights.

The Guidelines, however, emphasise turnover and employ a very mechanical approach to imposing fines. GDPR fines and other regulatory sanctions are not simply economic punishments or deterrents but form one part of what should be a framework for improving and enhancing the rights of individuals and delivering effective protection for them and their data. The heavy focus on turnover creates a misguided assumption of an increased culpability proportionate to the turnover number, without immediate regard for the nature and seriousness of the infringement or level of culpability.[3]

## II. Turnover, especially worldwide turnover, is not an appropriate measure for an assessment under Article 83 (2) GDPR and should not be the starting point for calculating a fine

The Guidelines provide for a completely new starting point for the calculation of fines by using a percentage of the legal maximum based on the annual global turnover. However, the turnover of an undertaking finds no mention in Article 83(2) of the GDPR. It should not be considered as a starting point for assessing a fine. While turnover is relevant to establishing the upper limit of a fine in Article 83 (4) and (5) GDPR, it is not foreseen in any of the factors in Article 83 (2) to also determine the starting point of the calculation. It would be disproportionate to employ an organisation's global turnover as a factor in establishing a starting point for calculating a fine where, for example, a GDPR violation relates only to the data of an organisation's employees in a specific member state. Similarly, where an infringement relates to a localised processing affecting very few individuals, it is debatable how global turnover would be appropriate and proportionate consideration to the violation. Even in competition law, which was the inspiration for the GDPR fines, the turnover calculation is linked to the relevant market[4] in line with proportionality considerations.

Some factors to be considered under GDPR Article 83(3) might be exacerbated or affected by the size of an undertaking—for example, financial benefits or losses avoided, which is foreseen by Article 83(2)(k)—the size and turnover *per se* are not a relevant consideration in setting a starting point for a fine. A contrary interpretation finds no basis in the GDPR and cannot be reconciled with the text of the law. And while Articles 83(4) and 83(5) permit assessments of fines at substantial levels to deal with the most serious of cases, they also do not set out any authority for the proposition that "the larger the undertaking, the higher the fine must automatically be," without consideration for proportionality, the individual circumstances of the case, or (at the very least) the type of infringement, number of data subjects involved and the risks to individuals from the infringement. An emphasis on the turnover for calculating administrative fines does not lead to adequate results for serious GDPR breaches in small turnover companies as compared to minor GDPR breaches in high turnover companies.[5]

---

[3] This also forces the exclusion of natural persons as controllers or processors from the Guidelines and raises questions on how to assess fines for non-for-profit organisations.

[4] See Guidelines on the method of setting fines imposed pursuant to Article 23(2)(a) of Regulation No 1/2003, European Commission (2006/ C 210/02), available at https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A52006XC0901%2801%29.

[5] See case LG Bonn – 29 Owi 1/20. The case concerns a fine of EUR 9,550,000 imposed by the Federal Commissioner for Data Protection and Freedom of Information (BfDI) on a company due to a breach of Article 32(1) GDPR. The Regional Court in Bonn upheld the BfDI decision but reduced the fine to EUR 900,000 and stated in relation to fines based on the turnover of the organisation (para 107), that the calculation of fines method as

Moreover, the EDPB has been actively addressing the disparities that inevitably arise when multiple regulators consider the same subject matter. , The Guidelines do not address instances where several national supervisory authorities may be handling similar cases in parallel. It would clearly be disproportionate for several supervisory authorities to impose a significant fine based on the global turnover when dealing with a national case that affected only a relatively limited number of individuals in either country**.**

The Guidelines correctly list the criteria each supervisory authority must consider when assessing fines in accordance with GDPR Article 83(1)—namely, the criteria listed in Article 83(2) GDPR. These do not include the turnover of an organisation. Therefore, the EDPB should exclude from the Guidelines the turnover as a consideration for a starting point in calculating a fine.

## III. Ambiguities related to concepts of concurrent infringements, unity of conduct and multiple infringements under Article 83(3) GDPR

Article 83(3), which considers "the same or linked processing operations", deals with the issue of concurrence of laws in circumstances where the same or linked conduct infringes different legal provisions (unity of conduct). Once unity of conduct has been established, the Guidelines develop applicable rules in case the same conduct gives rise to multiple infringements and further differentiate between apparent concurrence of offences and ideal concurrence of offences. CIPL identified several issues with the approach taken by the Guidelines.

### 1. There should not be an assumption against coherent conduct

CIPL suggests re-evaluating the EDPB's interpretation of "linked processing operations" as referred to in Article 83(3) GDPR**.** Processing would be considered linked, where a close contextual, spatial and temporal link exists between the parts of the processing activity that would appear as one coherent conduct.[6]

The Guidelines suggest in paragraph 28 that: "A sufficient link should not be assumed easily in order for the supervisory authority to avoid infringement of the principles of deterrence and effective enforcement of European law." However, the question of whether processing operations are linked will be one of fact and should be undertaken from a neutral evaluation, not one weighed against the controller. The burden of proving an infringement rests with the supervisory authority, and, logically, the burden of proving that processing is not linked should also fall on the supervisory authority and form part of their assessment. Also, a presumption of innocence is enshrined in Article 48 of the Charter, and it should not be made to step aside for the sake of achieving a higher fine. Instead, the assessment should start from a neutral position, carefully weighing all the circumstances of the case the Guidelines correctly reference**.**

employed by the BfDI fails in the case of serious data protection infringements of companies with low turnover and minor data protection infringements of companies with high turnover.

[6] Article 83(3) GDPR states: "If a controller or processor intentionally or negligently, for the same or linked processing operations, infringes several provisions of this Regulation, the total amount of the administrative fine shall not exceed the amount specified for the gravest infringement".

### 2. More clarity is required in the sections on the apparent concurrence of offences

CIPL agrees with the Guidelines' premise that in a case of "apparent concurrence", where the application of one provision subsumes the applicability of another[7], a fine is to be calculated on the selected infringement, generally limited to the gravest offence, to observe principles of proportionality and *ne bis in idem*.[8] This conforms to general principles of (criminal) law, recognised by international law and common to the EU member states. One provision may be *lex specialis* to another and thereby displace the latter completely (principle of speciality); one provision may be (explicitly or implicitly) subsidiary to another one, whereby only the latter is to be applied (principle of subsidiarity); or a dominant provision may absorb an ancillary provision (principle of absorption). In such situations of 'apparent' or 'false concurrence', only one penalty determined by the dominant provision is applied.[9] However, the provisions in the Guidelines on speciality, subsidiary and consumption would greatly benefit from more clarity and some more concrete examples of these concepts in the direct context of GDPR infringements. Paragraph 33 will need further explanation, and there may also be some previously intended footnotes missing in paragraph 35 of the Guidelines.

## IV. Aggravating and mitigating circumstances

CIPL agrees with the EDPB's premise that aggravating and mitigating factors, as listed in Article 83(2), GDPR should be taken into consideration only once in the course of the assessment and all facts compiled during the investigation have to find considered. However, we suggest reassessing the suggested application of some of the listed criteria.

### a. Member State statutes of limitations for previous breaches have to be addressed

The GDPR does not include any statute of limitations. These do, however, exist in the Member States and should be given due consideration. It is not a matter of whether a prior infringement that took place "a long time ago" is relevant, as suggested by the Guidelines, but whether such an assessment can stand the test of the statute of limitations enacted by the Member States. While we recognise Article 83(2)(e) GDPR takes relevant previous infringements into consideration, the Guidelines should address the effect of Member States' limitations statutes and how they are to be harmonised with the GDPR provisions. Conversely, while we, of course, agree that compliance with the law is the baseline, it is not clear why the fact that a controller is a "first offender" cannot be a consideration for mitigating circumstances in some cases**.**

Until and when there will be a harmonised set of procedural rules at the EU level, the EDPB should provide more detailed guidance on the applicability of member state-level statutes of limitation to create a baseline and avoid fragmentation.

[7] By way of specialty, subsidiarity, or consumption.
[8] Verwaltungsgerichtshof Ra 2018/02/0123, para 7 notes that penalties are to be imposed simultaneously if someone has committed several administrative offenses through several independent acts or one act falls under several penalties that are not mutually exclusive.
[9] See also AG Tanchev, Case C-10/18P, Marine Harvest, paras 135, 137 and 140.

### b. Codes of conduct or approved certification mechanisms

Paragraphs 105 and 106 of the Guidelines suggest that supervisory authority need not take account of a sanction imposed by a monitoring body that monitors compliance with a code of conduct or certification mechanism. Yet, at the same time, the supervisory authority may consider the same breach of a code of conduct as an aggravating factor. Without the obligation to consider a previously imposed sanction, the supervisory authority is at liberty to fine an organisation that has already been sanctioned for the same conduct by the independent monitoring body. This would undermine the incentive for codes of conduct and certification mechanisms as important tools for data protection compliance and accountability. Sanctions imposed by monitoring bodies should therefore be taken into consideration.

### c. Actions taken by the controller or processor to mitigate damage

The Guidelines set out that actions taken to mitigate damage prior to a supervisory investigation can be considered mitigating factors. CIPL points out that this might create an advantage for an infringement with intent, where the infringer is aware of the infringement and can change course at any time, versus a negligent infringement, where the infringer is not yet aware. CIPL would propose to connect this mitigating factor to the time of awareness of the infringement rather than the commencement of an investigation.

## V. Corporate Liability cannot be concluded from GDPR Recital 150

When discussing the legal maximums of administrative fines, the Guidelines refer to Recital 150 GDPR, which references Articles 101 and 102 of TFEU for the understanding of the term "undertaking" used in Articles 83 (4) to (6) and then continue to draw the conclusion that the GDPR follows a principle of direct corporate liability. [10] Applying doctrines purely based on competition law to the GDPR ignores its rationale and structure**.** As mentioned above, it can be helpful to look towards other fields of law as long as the nature of the GDPR and its basis in Article 16 (1) TFEU are preserved – the GDPR is not competition law. Recital 150 merely explains how the notion of "undertaking" used in Article 83(4) to (6) GDPR to distinguish the different ceiling amounts set for "undertakings" and "persons that are not an undertaking" is to be interpreted. Specifically, in the GDPR, responsibility for compliance with the obligations imposed, and liability for sanctions, are determined by the concept of the "controller", i.e., the "natural or legal person […] which, alone or jointly with others, determines the purposes and means of the processing of personal data".[11] The controller has to ensure that all processing meets GDPR requirements, including – importantly – in its relationships with other legal persons that may belong to the same single economic unit.[12] The GDPR does not recognise a "Konzernprivileg", each part in a group of undertakings, as defined by Article 4 (19) GDPR, is individually responsible for the data processing they undertake. Thus, reference to the concept of undertaking in competition law as an interpretative aid cannot be the lever to fully import all competition law concepts into the GDPR

[10] This entails that: "<…> all acts performed or neglected by natural persons authorized to act on behalf of undertakings are attributable to the latter and are considered as an act and infringement directly committed by the undertaking itself."
[11] Article 4(7) GDPR.
[12] C-131/12, *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, para 38 and 83; Case C-210/16, *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH*, Opinion of Advocate General Bot, para 44.

and drastically expand corporate liability without an objective nexus between the conduct and the affected entities. Assessments must be made case by case with a careful consideration as to the controller of the processing under investigation.

### VI. Overall accessibility and clarity of the Guidelines must be improved

The Guidelines set out to provide "a clear and transparent basis for the supervisory authorities' setting of fines". However, CIPL finds these Guidelines are quite theoretical and not easily accessible for average controllers and processors.

While guidance on fining does not need to be so specific to "allow a controller or processor to make a precise mathematical calculation of the expected fine", controllers or processors need to be able to access relevant guidance without too many barriers, to have legal certainty and understand the processes that apply to them to exercise their rights of defence. In this case, the Guidelines build on an earlier Article 29 Data Protection Working Party document, which is, by contrast, an accessible, clear, non-legalistic guide.[13] We recommend the two papers be further integrated.

### VII. Accountability should be a strong mitigating factor when considering regulatory enforcement

While we understand that these Guidelines specifically address the calculation of administrative fines, we nevertheless note with concern that there is little consideration for the relevance of organisational accountability. Supervisory authorities should consider accountability and frameworks demonstrating an organisational commitment to legal compliance and beyond as mitigating factors. Accountable behaviour should actively be encouraged by explaining how it will factor into any assessment of infringement and how it will affect the regulatory response. Acts of non-compliance do not occur in a vacuum; they should be considered within the context of an organisation's wider data protection management program and any external certifications or adherence to a code of conduct. Where similar infringements with a similar impact are identified within two organisations, but one maintains a stringent data protection program and the other does not, the SA should consider the organisation's good faith efforts, which tried, albeit unsuccessfully in that instance, [14] to comply with the law. Even more so, an organisation's good faith effort should be considered when deciding whether to initiate any enforcement action in the form of a fine in the first instance. Indeed, the supervisory authority should consider the level of oversight that senior management provides with respect to data management and other elements of accountability, as advocated by the CIPL Accountability wheel. Strong internal accountability frameworks should be considered mitigating factors in the same way the Guidelines, in reverse, consider previous infringements potentially aggravating factors.

Additionally, incentivising accountability would result in data controllers investing in comprehensive data protection management programs beyond just legal compliance. CIPL has conducted a recent global survey to analyse how enforcement agencies, including but not limited to data protection

[13] *Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679*, 3 October 2017, Article 29 Data Protection Working Party, 17/EN WP 253.
[14] Centre for Information Policy Leadership, *Report of the CIPL Accountability Mapping Project*, 2020, available at https://www.informationpolicycentre.com/cipl-2020-accountability-mapping-report.html.

authorities, consider accountability frameworks in their enforcement practices. [15] This confirmed that the concept of enforcement for the majority of non-DPA agencies is expanding beyond prosecution and imposing fines and includes the use of soft intervention and tools to achieve the regulatory goals. Accountability is recognised as a mitigating factor in their enforcement actions. Data protection agencies are also trending in that direction according to the data. CIPL suggests including the presence of accountability and compliance frameworks, programs, tools and measures as a mitigating factor in the methodology of calculating administrative fines.

*CIPL is grateful for the opportunity to comment on key issues related to the Guidelines on calculating administrative fines under the GDPR.*

*We look forward to providing further input as the Guidelines are finalised.*

*If you would like to discuss any of these comments or require additional information, please contact Bojana Bellamy, bbellamy@HuntonAK.com, Markus Heyder, mheyder@HuntonAK.com, or Natascha Gerlach, ngerlach@HuntonAK.com.*

[15] Organizational Accountability in Data Protection Enforcement, How Regulators Consider Accountability in their Enforcement Decisions available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_white_paper_on_organizational_accountability_in_data_protection_enforcement_-_how_regulators_consider_accountability_in_their_enforcement_decisions__6_oct_2021__3_.pdf.