Centre for Information Policy Leadership
HUNTON

CIPL Response to the EDPB Guidelines 04/2026 on the Application of the Power to Impose Administrative Fines in Relation to Other Corrective Powers Under the GDPR

Centre for Information Policy Leadership (CIPL)

13 November 2026

CIPL Response to the EDPB Guidelines 04/2026 on the Application of the Power to Impose Administrative Fines in Relation to Other Corrective Powers Under the GDPR

The Centre for Information Policy Leadership (CIPL)[1] welcomes the opportunity to comment on the European Data Protection Board (EDPB) Guidelines 04/2026 on the application of the power to impose administrative fines in relation to other corrective powers under the GDPR (the "Guidelines"), adopted for public consultation on 17 September 2026.

CIPL supports the EDPB's commitment to a harmonised enforcement approach based on a common understanding and consistent application of the GDPR. We recognise the considerable work reflected in the Guidelines, and in particular the effort to integrate the substantial body of case law of the Court of Justice of the European Union (CJEU) that has developed since the adoption of Guidelines 04/2022 on the calculation of administrative fines under the GDPR (the "Calculation Guidelines").

Corrective powers are an important tool to bring processing into compliance, protect the rights of individuals and ensure trust in the free flow of data. In the corrective measure toolbox, administrative fines should be reserved as a measure of last resort, used where other corrective measures would not achieve that purpose. The choice between corrective powers in Article 58(2) GDPR is central to that objective. An effective and proportionate regulatory response, which uses the full range of available tools to achieve better outcomes for individuals, society and regulated organisations, remains crucial for the proper functioning of the GDPR.

CIPL has long advocated an approach to GDPR enforcement that is focused on outcomes: bringing processing into compliance, protecting individuals and encouraging responsible behaviour. Under this approach, the regulatory response is proportionate to the seriousness of the infringement and the conduct of the organisation, and demonstrated accountability is recognised and taken into account. Fines are one tool among several, and should not be considered the default position.[2]

CIPL set out this approach in its 2022 response to the draft Calculation Guidelines.[3] We emphasised the importance of a contextual rather than mechanical assessment, centred on the nature of the infringement rather than, for example, the size of the organisation, and called for accountability to be treated as a mitigating factor. This response also builds on CIPL's research into how regulators take organisational accountability into account in their enforcement decisions.[4]

---

[1] The Centre for Information Policy Leadership (CIPL) is a global privacy and data policy think tank within the Hunton law firm that is financially supported by the firm, 85+ member companies that are leaders in key sectors of the global economy, and other private and public sector stakeholders through consulting and advisory projects. CIPL's mission is to engage in thought leadership and develop best practices for the responsible and beneficial use of data in the modern information age. CIPL's work facilitates constructive engagement between business leaders, data governance and security professionals, regulators, and policymakers around the world. For more information, please see CIPL's website at www.informationpolicycentre.com. Nothing in this document should be construed as representing the views of any individual CIPL member company or Hunton. This document is not designed to be and should not be taken as legal advice.

[2] See C. Hodges, 'Delivering Data Protection: Trust and Ethical Culture' (2018) 4 *European Data Protection Law Review* 65; and CIPL, *Regulating for Results – Strategies and Priorities for Leadership and Engagement*, 2017, which draws on C. Hodges, *Law and Corporate Behaviour: Integrating Theories of Regulation, Enforcement, Compliance and Ethics* (Hart Publishing, 2015).

[3] CIPL Response to the EDPB Guidelines 04/2022 on the calculation of administrative fines under the GDPR, 24 June 2022.

[4] CIPL, *Organizational Accountability in Data Protection Enforcement – How Regulators Consider Accountability in their Enforcement Decisions*, October 2021; CIPL, *Report of the CIPL Accountability Mapping Project*, 2020.

Copyright © 2026 by the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

Building on these previous comments, CIPL respectfully identifies several areas where the draft Guidelines would benefit from further reflection and fine-tuning before their final adoption:

1) The relationship between administrative fines and the other corrective powers, so that the choice of measure reflects the graduated system established by the GDPR;
2) The assessment of negligence, so that culpability remains a meaningful precondition for the imposition of a fine;
3) The weighing of aggravating and mitigating factors, including due recognition of organisational accountability;
4) The reasoning expected in decisions imposing corrective measures;
5) The framing and use of compliance orders, limitations and bans;
6) The scope of the controller's liability for the conduct of others; and
7) The interplay with the Calculation Guidelines in light of the evolving case law.

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

I. A presumption in favour of fines does not reflect the GDPR's graduated system of corrective powers

CIPL agrees with the EDPB that the choice of corrective measure should be guided by the respective purposes of the powers in Article 58(2) GDPR, some of which restore compliance while others primarily pursue deterrence (paragraph 17 of the Guidelines), although, as set out below, deterrence is not unique to fines. However, the methodology in the draft Guidelines sets up a binary test. Where an infringement is "minor", a fine is, as a general rule, not imposed. Where it is not minor, there is a "strong presumption" to impose a fine (paragraph 57; see also paragraph 119). CIPL is concerned that this presumption has no basis in the GDPR and could, in practice, make a fine the default outcome of most investigations.

a) The GDPR does not establish a hierarchy among corrective measures

Article 83(2) GDPR provides that fines are imposed "depending on the circumstances of each individual case", in addition to or instead of the other corrective measures. Recital 129 requires each measure to be appropriate, necessary and proportionate. The CJEU has confirmed that supervisory authorities (SAs) enjoy discretion in choosing the measure that meets these requirements.[5] None of these provisions ranks fines above other measures or requires the addressee to rebut a presumption.

Paragraph 18 of the Guidelines states that fines must be effective, proportionate and dissuasive, and that it is dissuasiveness which indicates an additional or different purpose of fines compared with the other measures in Article 58(2) GDPR. However, dissuasiveness is not unique to fines, as the Guidelines themselves recognise by acknowledging the reprimand as a measure with a deterrent effect (paragraph 25).

In practice, other corrective measures may have an equal or greater impact on organisational behaviour. A reprimand, where published, may cause significant reputational harm; an order to communicate a personal data breach to data subjects may have a similar impact; and a compliance order with a specified deadline requires concrete changes to the processing within a set period. Unlike

[5] Judgment of the CJEU of 26 September 2024, *Land Hessen*, C-768/21, EU:C:2024:785, paragraphs 37 and 41 to 43.

Copyright © 2026 by the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

a fine, these corrective measures act directly on the processing concerned and on the position of the individuals affected. The objectives of the GDPR are therefore often better served by a response tailored to the circumstances of each case, rather than by a presumption in favour of fines.

The draft Guidelines themselves stipulate in paragraph 113 that, where several penalties are equally appropriate, the least onerous should be chosen, and Example 14 describes an infringement that is not minor for which a reprimand is the proportionate response. A strong presumption in favour of fining sits uneasily with both, and risks turning the proportionality assessment in Step 5 into a formality.

b) The concept of "minor infringement" is too narrow to carry the weight placed on it

Paragraph 56 describes a minor infringement as one that does not pose a significant risk to data subjects and *does not affect the essence of the obligation concerned*. Depending on how "affecting the essence" is understood, few infringements that lead to a formal decision are likely to meet this description in practice. Combined with the presumption, almost every finding would result in a fine, irrespective of the organisation's conduct, the harm caused, the clarity of the law or the remediation undertaken.

Paragraph 26 confirms that reprimands are "generally, but not necessarily only" available in the two cases mentioned in Recital 148 GDPR, and Example 14 shows that a reprimand can be the proportionate response to an infringement that is not minor. The Guidelines should build on this and make clear that the "minor" category does not mark the outer limit of the cases in which a fine can be dispensed with. A reprimand or order is likely to be sufficient, in particular where the degree of negligence is low, the infringement caused no or limited harm, the legal position was uncertain at the time of the conduct, the organisation remediated promptly and effectively, or the infringement is an isolated failure within a mature accountability programme. As most of the current examples of minor infringements concern SMEs and non-profit organisations, examples involving larger organisations would also be helpful.

This is particularly relevant for personal data breaches notified by the controller. Many investigations begin only because a controller has notified a breach to the SA, as Article 33 GDPR requires. Where the controller has also cooperated with the SA and taken effective remedial action, a reprimand or order will often be an adequate response, even where the infringement is not minor. A strong presumption in favour of fines risks placing controllers that comply with their notification obligations in a worse position than those whose comparable shortcomings are never reported. Examples 11 and 13, which both concern breaches, appear only in the section on minor infringements. CIPL suggests adding an example of a notified breach that is not minor, but for which a reprimand or order would nevertheless be the proportionate response.

c) Dissuasiveness should be assessed in the individual case

Paragraph 112 states that SAs should "establish and maintain a practice of imposing administrative fines" to achieve general deterrence. While fines play an important role when it comes to the egregious infringements and repeat offenders, fines do not, in themselves, bring processing into compliance or remedy the position of affected individuals. Effectiveness of enforcement should not be measured by the size of the fines imposed, but by the changes in practice it achieves. Article 83(1) GDPR requires each fine to be effective, proportionate and dissuasive "in each individual case"; general deterrence cannot, in itself, justify a fine that the circumstances of the case would not otherwise warrant.

Copyright © 2026 by the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

Effective deterrence also derives from the certainty and visibility of enforcement action, including published reprimands and binding orders.[6] A default towards fines may weaken the very incentives the GDPR seeks to create: to self-report, to engage early with SAs and to remediate during an inquiry. Organisations are more likely to do so where they can expect this to be reflected in the outcome.

CIPL therefore suggests that the EDPB reconsider the presumption in paragraphs 57 and 119 and instead treat fines as a measure with a higher bar, reserved for egregious infringements, repeat offenders and cases where other corrective measures would not be sufficient to bring the processing into compliance or to deter recurrence.

II. The negligence threshold should not result in de facto strict liability

1) Fines are punitive, and the associated safeguards apply

The Guidelines acknowledge that GDPR fines meet the so-called *Engel* criteria (footnote 8). This is the test developed by the European Court of Human Rights, and applied by the CJEU, to determine whether a sanction is criminal in nature, regardless of how it is labelled in national law. CIPL agrees and considers that this acknowledgement has important consequences that the Guidelines should further address in their discussion of negligence and intent.

When a sanction is criminal in nature, the fundamental safeguards of criminal law apply. These include the presumption of innocence (Article 48 of the EU Charter of Fundamental Rights) and the principle that a penalty may only be imposed for conduct which could reasonably have been known to be unlawful at the time it took place (Article 49(1) of the Charter). In practice, this means that it is for the SA to establish that the organisation acted at least negligently, separately for each infringement and on the basis of concrete facts, and not for the organisation to prove that it did not. The mere fact that an infringement occurred and was not intentional should not lead automatically to a finding of negligence. This concern is heightened by paragraph 49, which, citing Advocate General Emiliou, describes the threshold for negligence as so low that it is difficult to envisage situations where it is not satisfied. Read together with paragraph 50, this risks turning culpability into a formality and negligence into de facto strict liability, even though the CJEU has made clear that a fine may only be imposed for an infringement committed intentionally or negligently.[7]

2) EDPB guidelines should not consider errors "always" avoidable

The Guidelines state that, where EDPB (non-legally binding) guidelines exist, an organisation's error is always to be considered avoidable and therefore at least negligent (paragraph 50). EDPB guidelines are a valuable source of clarity on how the law should be interpreted. However, they are not legally binding; the CJEU has the final word on the interpretation of the GDPR, and the Court has, on occasion,

[6] See CIPL, *Regulating for Results – Strategies and Priorities for Leadership and Engagement*, 2017; CIPL, *Getting the Best Outcomes: Pathways for Data Protection and Privacy Authorities*, 2024, available at https://www.informationpolicycentre.com/wp-content/uploads/2024/10/cipl_getting_the_best_outcomes_oct24-1.pdf.

[7] Judgment of the CJEU of 5 December 2023, *Deutsche Wohnen*, C-807/21, EU:C:2023:950, paragraph 75; Judgment of the CJEU of 5 December 2023, *Nacionalinis visuomenės sveikatos centras* (*NVSC*), C-683/21, EU:C:2023:949, paragraph 80.

Copyright © 2026 by the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

taken a different view from that of individual SAs.[8] Guidelines also evolve, including between their draft and final versions. They are also often detailed and layered, and can reasonably be read in more than one way.

Paragraph 50 does not state expressly that it refers only to guidelines in force when the organisation acted, and the Guidelines should make this clear. Negligence must be judged by what an organisation could have known at the time it acted: guidance or interpretations adopted afterwards cannot show that it should have known better. CIPL further suggests that the EDPB treat the existence of guidelines as one relevant factor in assessing negligence, rather than as conclusive, and only where final guidelines on the specific issue were in force at the time of the conduct.

3) Documented legal assessments reflect accountability, not negligence

The GDPR is a principles-based framework. The accountability principle (Articles 5(2) and 24 GDPR) expects organisations to make and document their own assessments, including legitimate interest assessments and data protection impact assessments.

Examples 4a and 4b suggest that a documented, good-faith assessment which considers contrary views and reaches a reasoned conclusion is itself evidence of negligence. This risks discouraging the internal analysis that accountable organisations conduct. Such an assessment should, at a minimum, be relevant to the degree of negligence under Article 83(2)(b) GDPR and to the choice of corrective measure. CIPL agrees in principle with Example 4c that advice which is undocumented or accepted without scrutiny should carry less weight. However, an organisation should be able to demonstrate that it acted diligently without having to waive legal privilege, for example by describing the question on which advice was sought, the facts provided and when the advice was obtained. As drafted, Example 4c could put pressure on organisations to disclose privileged advice and, in turn, discourage them from seeking it.

4) The minimum degree of negligence should not be counted as aggravating

CIPL welcomes the distinction drawn in paragraphs 71 and 72 between different degrees of negligence. Since negligence is a minimum precondition for any fine, and its threshold is described as low, the initial finding of negligence should be neutral when assessing whether an infringement is minor. Only features of the conduct that go beyond the minimum required to establish culpability, such as a high degree of negligence or intent, should weigh in favour of a fine, and the SA should identify them.

III. Aggravating and mitigating factors should be applied in a balanced manner

1) Accountability should be a strong mitigating factor

As CIPL emphasised in its 2022 response, acts of non-compliance do not occur in a vacuum. They should be considered in the context of an organisation's wider data protection management programme, including senior management oversight, risk assessment, training, monitoring and the role of the Data Protection Officer, as well as any adherence to codes of conduct or certifications. Where two organisations commit similar infringements with similar impact, but one maintains a

[8] See, for example, Judgment of the CJEU of 4 October 2024, *Koninklijke Nederlandse Lawn Tennisbond*, C-621/22, in which the Court confirmed that a purely commercial interest can constitute a legitimate interest, contrary to the position previously taken by the Dutch SA.

Copyright © 2026 by the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

robust accountability programme, and the other does not, their degree of responsibility under Article 83(2)(d) GDPR is not the same. CIPL's research has shown that many enforcement bodies, within and beyond data protection, already recognise accountability as a mitigating factor.[9]

Paragraph 77 currently limits the mitigating effect of such measures to exceptional circumstances where the organisation has gone "above and beyond" its obligations. An organisation that has invested in demonstrable, robust and effective accountability measures should be considered to meet that threshold. Robust privacy management programmes[10], as well as proactive engagement with SAs that goes beyond the duty to cooperate under Article 31 GDPR, should be considered mitigating, and are particularly relevant when deciding whether a fine is necessary at all. This would also encourage organisations to invest in accountability beyond the legal minimum.

2) Previous infringements and first offenders

CIPL agrees that previous infringements can be a relevant factor and welcomes the recognition that their significance diminishes over time (paragraph 81). Three clarifications would, however, be helpful. First, only infringements established in decisions that have become final, i.e. are no longer subject to appeal, should be taken into account, since an infringement under appeal may still be annulled. Second, paragraph 80 states that previous infringements of a different subject matter may be relevant because they "could be indicative of a general level of insufficient knowledge or disregard" for the data protection rules. Rather than presuming such a link, the SA should explain in each case why an earlier infringement on a different subject is relevant. Third, as CIPL noted in 2022, national limitation periods must be respected. Paragraph 82 acknowledges such rules, as well as national record-deletion obligations, and a common approach to them would avoid fragmentation.

Conversely, while CIPL agrees that compliance with the law is the baseline (paragraph 88), it does not see why the absence of previous infringements cannot be taken into account in some cases, as CIPL also argued in 2022. A long record without infringements is relevant, for example, when considering whether a fine is needed for specific deterrence. Example 6 of the Guidelines itself counts the absence of similar past incidents among the mitigating facts.

3) Actions taken to mitigate damage

Paragraph 74 gives greater weight to measures taken before the commencement of the SA's investigation became known to the controller or processor. CIPL reiterates the proposal made in its 2022 response to connect this factor to the time the organisation became aware of the infringement. Measures taken during an inquiry should be taken into account in proportion to their effectiveness, both when deciding whether to impose a fine at all and, where one is imposed, when setting its amount, even where they do not remove every consequence for every individual. Denying credit for such measures could discourage organisations from improving their practices while an inquiry is ongoing.

---

[9] CIPL, *Organizational Accountability in Data Protection Enforcement – How Regulators Consider Accountability in their Enforcement Decisions*, October 2021.
[10] See CIPL, *The Case for Accountability: How it Enables Effective Data Protection and Trust in the Digital Society*, July 2018; CIPL, *Incentivising Accountability: How Data Protection Authorities and Law Makers Can Encourage Accountability*, July 2018; and CIPL, *Report of the CIPL Accountability Mapping Project*, 2020.

Copyright © 2026 by the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

4) Cooperation and compliance with previous measures

CIPL agrees that the duty to cooperate under Article 31 GDPR is mandatory. However, cooperation going beyond that minimum, such as proactively proposing and implementing compliance changes, or consulting the SA before implementing changes, should be recognised under Article 83(2)(f) GDPR without requiring evidence of an exceptional reduction in harm. Similarly, Article 83(2)(i) GDPR expressly lists compliance with previously ordered measures as a factor, yet paragraph 99 gives such compliance no weight unless the organisation goes beyond what was ordered. Full and timely compliance should be capable of being taken into account, rather than being relevant only when lacking.

5) Codes of conduct and certification mechanisms

Paragraph 103 provides that the SA is not obliged to take account of sanctions imposed by a monitoring body under a code of conduct. CIPL raised the same issue in relation to the Calculation Guidelines in 2022. Without an obligation to consider such sanctions, an organisation may be sanctioned twice for the same conduct, which would undermine the incentive to adhere to codes of conduct and certification mechanisms as important accountability tools. CIPL suggests that SAs be required to take such sanctions into account.

6) Each factor should be taken into account only once

CIPL welcomes the statement in paragraph 100 that the same non-compliant behaviour cannot be punished twice, and recalls that the Calculation Guidelines also recognise that each factor should be considered only once. CIPL suggests that the Guidelines state this as a general principle, applying both across the Article 83(2) factors and across infringements found under different provisions on the basis of the same conduct. For example, the categories of personal data concerned may inform the assessment of gravity under Article 83(2)(a) GDPR or be considered under Article 83(2)(g) GDPR, but should not be counted twice.

IV. Decisions to impose fines must be fully reasoned

CIPL welcomes paragraph 12 of the Guidelines, which confirms that SAs remain bound by the duty to state reasons and that a mere reference to the Guidelines cannot replace case-specific reasoning. However, paragraph 10 states that SAs are not obliged to provide reasoning on aspects that are not applicable, "in particular with respect to the various factors as listed in Article 83(2) GDPR". This statement could be read as allowing SAs to set aside factors, including mitigating factors raised by the addressee, without providing transparency over the decision-making.

Article 83(2) GDPR requires that due regard be given to each listed factor. Given the punitive nature of fines, the right to good administration (Article 41 of the Charter), the right to an effective remedy (Article 47 of the Charter) and the procedural safeguards required by Article 83(8) GDPR call for reasoning that enables the addressee to understand the decision and a court to review it. Without transparency, neither the addressee nor ultimately a court can assess to what extent a factor was considered and rejected, or possibly overlooked.

The decision should provide insight into why a fine is necessary in addition to, or instead of, the other corrective measures, and how those other measures were taken into account. Since the conclusions on the Article 83(2) factors are reused when calculating the fine (paragraph 10), transparency on the

Copyright © 2026 by the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

weight given to each factor also supports consistency between SAs, which is the very objective of the Guidelines.

Finally, in cross-border cases, the intended corrective measures may change between the preliminary findings, the draft decision and the final decision, including following the dispute resolution procedure under Article 65 GDPR. The GDPR Procedural Regulation gives parties the right to be heard on the preliminary findings, including the intended corrective measures.[11] CIPL suggests that the Guidelines confirm that, where a new or materially increased measure is introduced at a later stage, the party is informed of the change and its reasons and given the opportunity to comment.

V. Orders and bans should be specific, necessary and proportionate

1) Compliance orders

Article 58(2)(d) GDPR allows SAs to order that processing be brought into compliance "where appropriate, in a specified manner and within a specified period". An order expressed only in general terms leaves the addressee uncertain about what is required, and makes it difficult to demonstrate compliance or to assess later non-compliance under Articles 83(2)(i) and 83(6) GDPR. The Guidelines should confirm that orders identify the required outcome with sufficient precision to be implemented and verified, within a realistic time period.

An order should also be *necessary*. In *Land Hessen*, the CJEU accepted that an SA may refrain from adopting a corrective measure where the controller has already brought the infringement to an end and ensured that it will not recur.[12] By the same reasoning, an order adds little where the processing has ceased or has already been brought into compliance, and the SA has no reason to doubt this. CIPL suggests that the Guidelines reflect this.

2) Limitations and bans

A definitive limitation or ban under Article 58(2)(f) GDPR is among the most intrusive measures available. Paragraph 33 indicates that a permanent measure may follow other measures where those cannot restore the legal situation. CIPL suggests making this principle explicit: a definitive ban should be reserved for cases where an order to bring processing into compliance, or another less intrusive measure, cannot achieve lawful processing.

Where an SA imposes both an order to bring processing into compliance and a limitation or ban addressing the same deficiency, it should explain why both are necessary. Where a temporary limitation is imposed in a final decision, it should be linked to clear conditions for lifting it, consistent with the approach described for suspension orders in paragraph 29.

3) The controller's liability should be confined to its own conduct

In its 2022 response, CIPL cautioned against importing competition law concepts of corporate liability into the GDPR without regard to its structure, in which responsibility attaches to the controller. The CJEU has since confirmed in *Deutsche Wohnen* that a legal person is directly liable for infringements

[11] Regulation (EU) 2025/2518 of the European Parliament and of the Council of 26 November 2025 laying down additional procedural rules on the enforcement of Regulation (EU) 2016/679, Article 19.
[12] *Land Hessen*, paragraphs 41 to 43.

Copyright © 2026 by the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

committed by persons acting on its behalf, without the need to identify a specific individual.[13] CIPL takes this into account. The underlying principle nevertheless remains: liability under the GDPR follows the roles and obligations of the controller and processor.

CIPL welcomes paragraph 42 of the Guidelines, which reflects *NVSC*. A controller is not liable for a processor's conduct where the processor processes data for its own purposes or in a manner incompatible with the framework set by the controller; in such cases, the processor becomes a controller under Article 28(10) GDPR.[14]

Paragraph 43 adds that, even where attribution is disrupted, the controller may be separately liable, for example under Article 32 GDPR, for not having implemented measures against such conduct. CIPL agrees that a controller remains responsible for its own obligations. However, the paragraph should make clear that this concerns a separate infringement, which must be established on its own terms, together with the controller's own culpability. Otherwise, it risks reintroducing through Article 32 GDPR the attribution that *NVSC* excludes. In particular, the CJEU has held that unauthorised disclosure or access is not in itself sufficient to conclude that the controller's technical and organisational measures were inappropriate.[15] The assessment must therefore focus on the measures themselves, in light of the risks known at the time, and not be made with hindsight.

Similarly, CIPL accepts that an employee's failure to follow instructions does not necessarily break the controller's liability (paragraph 41).[16] Where an organisation had clear instructions, training and controls in place, and an individual deliberately circumvented them, this should nevertheless be reflected in the degree of responsibility under Article 83(2)(d) GDPR and in the choice of corrective measure. Example 11 illustrates this approach well, and CIPL suggests reflecting the principle in the text.

Finally, paragraph 45 refers to national rules extending liability for payment of a fine, including to parent companies. CIPL suggests clarifying that such rules concern the recovery of a fine imposed on the liable controller or processor, and do not make other group entities addressees of the finding of infringement.

VI. Interplay with the Calculation Guidelines and the evolving case law

The Guidelines complement the Calculation Guidelines, and the conclusions reached on the Article 83(2) factors when deciding whether to impose a fine are reused when calculating it (paragraph 10). The concerns CIPL raised in 2022 on the calculation methodology are therefore directly relevant to these Guidelines.

1) Turnover should not determine whether a fine is imposed

In 2022, CIPL argued that turnover is not among the criteria listed in Article 83(2) GDPR and should not drive the calculation of a fine. Since then, the CJEU has confirmed that, where the addressee forms part of an undertaking, the maximum fine is based on the turnover of that undertaking, and that its economic capacity may be relevant when setting the amount.[17] CIPL takes these rulings into account.

---

[13] *Deutsche Wohnen*, paragraphs 44 and 46.
[14] *NVSC*, paragraph 85.
[15] Judgment of the CJEU of 14 December 2023, *Natsionalna agentsia za prihodite*, C-340/21, EU:C:2023:986.
[16] Judgment of the CJEU of 11 April 2024, *juris*, C-741/21, EU:C:2024:288, paragraph 51.
[17] *Deutsche Wohnen*; Judgment of the CJEU of 13 February 2025, *ILVA*, C-383/23, EU:C:2025:84.

Copyright © 2026 by the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

They concern the ceiling and calibration of a fine, however, not whether a fine should be imposed at all. That decision should rest on the conduct and the Article 83(2) factors. CIPL suggests that the Guidelines state expressly that the size of an organisation does not, by itself, weigh in favour of a fine rather than another corrective measure. Where turnover subsequently affects the amount, its effect should be disclosed and reasoned.

2) Concurrent infringements and the overall response

In 2022, CIPL called for more clarity on concurrent infringements and on the application of Article 83(3) GDPR to the same or linked processing operations. The Guidelines do not address how the decision to fine should take account of several infringements arising from the same conduct, or of other corrective measures imposed at the same time. CIPL suggests that, in Step 5, the SA assess whether the overall response is effective, proportionate and dissuasive, considering together all fines and other measures relating to the same or linked processing operations, and respecting the principle of *ne bis in idem*.

3) Duration of proceedings

Inquiries in complex cases may last several years. CIPL suggests that the Guidelines confirm that the length of proceedings should not, of itself, operate to the detriment of the addressee, consistent with the duty to act within a reasonable time. Where, for instance, the turnover figure relied upon differs significantly from that during the period of the infringement, the SA should explain the effect of this choice.

4) Review in light of the case law

The case law on GDPR fines continues to develop, and the Irish High Court has recently referred questions on fining methodology to the CJEU.[18] CIPL welcomes the EDPB's commitment to regularly review the Guidelines (paragraph 13), and encourages it to review the Imposition and Calculation Guidelines together once the Court has ruled, with a further opportunity for stakeholder input.

[18] *TikTok Technology Limited v Data Protection Commission* [2026] IEHC 419 (judgment of 30 June 2026).

Copyright © 2026 by the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.

VII. CIPL recommendations

The EDPB should consider:

- Replacing the "strong presumption" to impose a fine for infringements that are not minor with an approach in which fines are imposed only where other corrective measures would not achieve compliance.
- Recognising that reprimands and orders can be the appropriate means of achieving compliance, also for infringements that are not minor, in particular where negligence is low, harm is limited, the legal position was uncertain, or the organisation remediated promptly.
- Including an example of a notified personal data breach that is not minor, but for which a reprimand or order is the proportionate response.
- Removing language suggesting that negligence will almost always be established, or that an error is "always" avoidable where EDPB guidelines exist.
- Clarifying that guidance or interpretations adopted after the relevant conduct cannot by themselves establish negligence.
- Recognising documented, good-faith legal assessments as relevant to the degree of negligence and the choice of corrective measure, without requiring organisations to waive legal privilege.
- Including demonstrable accountability measures, codes of conduct and certifications as mitigating factors, and allowing a clean compliance record to be taken into account.
- Assessing remedial measures from the time the organisation becomes aware of the infringement, rather than from the start of an investigation.
- Requiring SAs to take into account sanctions already imposed by a code of conduct monitoring body.
- Ensuring that the same conduct or circumstance is taken into account only once.
- Requiring a brief, reasoned position on each Article 83(2) factor, and an explanation of why a fine is necessary in light of the other measures imposed.
- Clarifying that compliance orders should be specific and necessary, and that definitive bans are a measure of last resort.
- Confining the controller's separate liability under paragraph 43 to its own, separately established infringement.
- Confirming that the size of an organisation does not by itself justify imposing a fine, and reviewing the Imposition and Calculation Guidelines together in light of pending CJEU references.

Copyright © 2026 by the Centre for Information Policy Leadership at Hunton Andrews Kurth LLP.