Consultation questions: Data Protection Fining Guidance

Start date: 2 October 2023

End date: 27 November 2023

About you

Your name:

[redacted]

Email address:

[redacted]

If you are responding on behalf of an organisation, please tell us the name of the organisation, your role and (if applicable) how the views of the members of the organisation have been obtained:

Amazon

If you are responding as an individual, please tell us if you are responding in a professional or private capacity:

N/a

If you are responding as an individual, please tell us if you consent to us publishing your name alongside your response (we will otherwise publish your response anonymously):

N/a

Our questions

Answers to the following questions will be helpful in finalising the draft Data Protection Fining Guidance. You do not need to answer all the questions.

The headings refer to the relevant sections of the draft Data Protection Fining Guidance.

Statutory Background

1. Do you have any comments on our approach to the concept of an 'undertaking' for the purpose of imposing fines?

Thank you for the opportunity to provide feedback on the Draft Guidance.

We note that the ICO proposes to define 'undertaking' under Article 83(4) to (6) of the UK GDPR in light of Recital 150 (i.e. as within the meaning of Articles 101 and 102 TFEU). We appreciate that the EU's collective of national data regulators has endorsed the vast body of CJEU case law on the definition of 'undertaking' for the purpose of setting fines to date. We broadly agree with the ICO's proposal to follow this principle. We also note that this is subject to review by the EU courts[1].

In considering the definition of 'undertaking' for the purpose of imposing fines, we would welcome the ICO's views on the following:

Further clarity on the meaning of 'economic, organisational and legal links'

The Draft Guidance adopts the concept of 'decisive influence' to determine if a group of entities are jointly part of an undertaking. This is a concept borrowed from settled CJEU and UK competition case law and which the EDPB considers to apply equally to the GDPR.

The EDPB's view is that the applicable test to determine whether two or more entities form a single economic unit depends largely on whether (i) the individual entity is free in its decision-making ability, or (ii) a leading entity, namely the parent company, exercises decisive influence over the others, based on the 'economic, legal and organisational links'[2] between the parent company and its subsidiary – taken into account at paragraph 29 of the Draft Guidance.

We would welcome further detail from the ICO on what 'economic, legal and organisation links' would be deemed by the ICO as (i) tying a subsidiary to its parent, and / or (ii) acting independently from its parent. It would be particularly helpful for the ICO to give practical examples referencing the GDPR (e.g. whether the parent exercises decisive influence over the processing activity, control over general GDPR compliance, power to instruct a subsidiary on the use of global policies, etc).

'Decisive influence' in the GDPR context

We would welcome the ICO's views on the broader question of whether the concept of 'decisive influence' should be construed in the UK GDPR context. We understand that the EDPB's view is that, for the purpose of establishing whether a parent company exercises decisive influence over others in the group, the 'decision-making ability' relates to the conduct of the subsidiary 'on the market'[3]. For example, how the subsidiary organises its affairs, day-to-day business and strategic decisions, and not simply limited to the specific data processing activities[4].

---

[1] *Anklagemyndigheden v ILVA A/S* (Case C-383/23) ("**ILVA**"). On 21 June 2023 a Danish Court lodged with the CJEU two questions for preliminary ruling: (i) *"must the term 'undertaking' in Article 83(4) to (6) of the GDPR must be understood as an undertaking within the meaning of Articles 101 and 102 TFEU, in conjunction with recital 150 of that regulation, and the case-law of the CJEU concerning EU competition law"*; and if so, (ii) *"must Article 83(4) to (6) of the GDPR be interpreted as meaning that…regard must be had to the total worldwide annual turnover of the economic entity of which the undertaking forms part, or only the total worldwide annual turnover of the undertaking itself?"*

[2] *Akzo Nobel and Others v Commission* (T-175/05) [2009] is the source of this phrase in the 'undertaking' test. See also *Durkan Holdings v Office of Fair Trading* (1121/1/1/09) [2011].

[3] Guidelines 04/2022 on the calculation of administrative fines under the GDPR ("**EDPB Guidelines**"). See paragraph 122, footnote 54.

[4] Decision on DPC Inquiry IN-20-8-1, Inquiry concerning data transfers from the EU/EEA to the US by Meta Platforms Ireland Limited for its Facebook service, issued 12 May 2023. See paragraph 9.122.

In a competition law context, an entity's wider behaviour 'on the market' may be intrinsically linked to the anti-competitive conduct. However, from a UK GDPR perspective, an entity's breach may have nothing to do with its other behaviour 'on the market', and hence it might be more reasonable to tie the control test more closely to the relevant wrongdoing (e.g. by focusing on the parent's control over the specific processing activities concerned, and / or control over broader GDPR compliance).

For example, consider a parent company that controls its subsidiary's commercial activities (e.g. a recent strategic merger), but has no oversight or day-to-day decision-making powers over the specific processing activities that the subsidiary undertakes, e.g. the subsidiary may have dedicated business teams that exert control over the business-related processing activities, or they may have an entirely separate HR function that runs their employee processing independently. If the 'decisive influence' test was applied through a UK GDPR lens, it could make a material difference in the outcome of the assessment.

The EDPB have so far not taken this view, but we would be interested to understand the ICO's view on this point. This approach would in principle require the ICO to consider the question of what 'market behaviour' means in the UK GDPR context, and provide very specific examples and guardrails.

2. Do you have any comments on our approach to fines where there is more than one infringement by an organisation?

The Draft Guidance provides valuable information on the ICO's methodology for identifying the appropriate statutory maximum for fines when there are multiple alleged breaches of GDPR provisions. The proposed explanations on how the ICO distinguishes between 'same or linked' conduct and separate conduct are helpful. However, the Draft Guidance is unclear as to how the ICO would determine the appropriate statutory maximum when multiple infringements associated to the same or linked conduct arise.

We would welcome clarification on how the ICO would decide the statutory maximums in these circumstances, for example: (i) a single action gives rise to more than one identical infringement; (ii) a single action gives rise to fully overlapping infringements; and (iii) a single action gives rise to partly overlapping infringements. We recognise that the ICO has previously encountered (iii) in the 2016 British Airways Penalty Notice[5] and the 2020 Marriott International Inc Penalty Notice[6], where the ICO found breaches of both Article 5(1)(f) GDPR's general data security principle and Article 32 GDPR's specific obligation to implement appropriate security measures, and found that Article 32 did not override the basic requirements laid down in Article 5(1)(f).

The UK GDPR does not envision this range of circumstances, so we would welcome further clarity through the Draft Guidance.

3. Do you have any other comments on the section on 'Statutory Background'?

No further comments.

[5] British Airways plc Penalty Notice. See paragraphs 7.77 to 7.83.

[6] Marriott International Inc. Penalty Notice. See paragraphs 7.83 to 7.86.

Circumstances in which the Commissioner would consider it appropriate to issue a penalty notice

4. Do you have any comments on our approach to assessing the seriousness of an infringement?

See Question 7 below.

5. Do you have any comments on our approach to assessing relevant aggravating and mitigating factors?

See Question 7 and 10 below.

6. Do you have any comments on our approach to assessing whether imposing a fine is effective, proportionate and dissuasive?

No comments.

7. Do you have any other comments on the section on 'Circumstances in which the Commission would consider it appropriate to issue a penalty notice'?

We recognise and welcome the thoroughness and thought that has gone into the Draft Guidance on this section. It helpfully describes each Article 83(2) UK GDPR factor in detail and gives clarity on the ICO's specific considerations for deciding when it would be appropriate to issue a penalty notice.

As the ICO has identified in the Draft Guidance, Article 83(2) makes it clear that there are two stages to consider when issuing a penalty notice: (i) whether a fine should be imposed (the "**Review Stage**"); and (ii) the amount of the fine (the "**Calculation Stage**"). This two-stage approach aligns with the ICO's current Regulatory Action Policy (the "**RAP**")[7] and the Article 29 Working Party Guidelines on the application and setting of administrative fines as endorsed by the EDPB (the "**WP29 Guidelines**")[8].

During the Review Stage, our understanding is that the factors in Article 83(2)(a) to (k) should be considered in turn and together as a whole when deciding whether to issue a penalty notice. This approach has been adopted by the ICO[9] and the Irish DPC's[10] recent decisions against TikTok, the Italian Garante's decision against Axpo Italia[11], and the Irish DPC[12] and EDPB's findings against Meta, where the EDPB first considered factors (a) to (k) in turn before concluding that "*the overall analysis of the relevant factors listed in Article 83(2) GDPR demonstrates the need to impose an administrative fine*".

---

[7] Regulatory Action Policy ("**RAP**"). See page 24.

[8] Article 29 Working Party, Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679 ("**WP29 Guidelines**"), adopted on 3 October 2017 (WP 253), endorsed by the EDPB on 25 May 2018. See page 9.

[9] TikTok Information Technologies UK Limited and TikTok Inc (TikTok) monetary penalty notice ("**ICO TikTok MPN**"), issued 15 May 2023. See Section V from paragraph 190.

[10] Decision on DPC Inquiry IN-21-9-1, In the matter of TikTok Technology Limited, issued 15 September 2023. See paragraph 311, where the Commissioner stated: *"The decision as to whether to impose an administrative fine in respect of an infringement is a cumulative decision which is taken having had regard to all the factors as set out in Article 83(2)(a) to (k) GDPR. Therefore, I will now proceed to consider each of these factors in turn…"*

[11] GPDP Measure of 28 September 2023 [9940988] (only available in Italian). See Section 6 where the Article 83(2) factors were considered in no particular order.

[12] Decision on DPC Inquiry IN-20-8-1.

In the Draft Guidance, however, the ICO seems to be suggesting to first have regard to the factors listed in Article 83(2)(a), (b) and (g) (regarded as "*the seriousness of the infringement(s)*); then consider the remaining factors under Article 83(2) (regarded as "*aggravating or mitigating factors*"); and finally consider whether imposing a fine would be effective, proportionate and dissuasive[13].

We suspect that this proposed grouping of the Article 83(2) factors takes inspiration from EDPB Guidelines 04/2022 on the **calculation** of administrative fines (the "**EDPB Guidelines**")[14]. We appreciate that the ICO may have intended to replicate this structure across the Review and Calculation Stages to define the concepts of 'the seriousness of the infringement' and 'relevant aggravating or mitigating factors' in the Review Stage, before reusing them in the Calculation Stage. If this is what the ICO intended, we are concerned that this proposed format risks: (i) creating confusion between the Review and Calculation Stages; and (ii) in any event represents a departure from the current approaches of the EDPB[15] and other supervisory authorities, including the ICO itself.

We welcome the additional detail and clarification provided by the proposed subsections on the interpretation and application of the Article 83(2) factors, but we would request that the ICO simplifies the structure of this section to align with current practice of supervisory authorities in considering each of the Article 83(2) factors holistically. We believe this would provide the ICO with a greater degree of flexibility to pursue a risk-based approach that considers all the circumstances.

[13] See paragraphs 54-72, 73-101, and 102-105 of the Draft Guidance, respectively.

[14] EDPB Guidelines. See paragraph 17.

[15] EDPB Binding Decision 1/2023. See paragraphs 169-172, where it is only after the decision to issue a fine is made, does the EDPB reference the EDPB Guidelines and identify Article 83(2)(a), (b), and (g) as part of 'the seriousness of the infringement' to inform the appropriate starting amount of the fine.

Calculation of the appropriate amount of the fine

8. Do you have any comments on calculating the starting point for the fine based on the seriousness of the infringement?

We understand that the ICO currently follows the five-step mechanism set out in the RAP to calculate the penalty amount[16]. However, from the ICO's recent decisions (e.g. TikTok[17] and Clearview AI[18]), we see that the RAP has its challenges. In particular: (i) the "initial element removing any financial gain" in Step 1 can often be difficult to determine[19] [20]; and (ii) in many cases no further adjustments were made in Steps 3-5 as all relevant aggravating and mitigating factors, as well as deterrence, have already been considered in Step 2[21]. We therefore understand and welcome the ICO's review of this calculation process as part of the Draft Guidance.

The Draft Guidance proposes a new five-step approach in paragraph 106. As noted in our response to Question 7 above, we understand that *Step 1 (as proposed)* considers Article 83(2)(a), (b), and (g) to determine '*the seriousness of the infringement*'. The level of seriousness then informs the starting point as a percentage of the relevant applicable statutory maximum fine[22]. The remaining factors under Article 83(2) are then considered as '*aggravating or mitigating factors*' in *Step 4 (as proposed)* and may increase or decrease the fine relative to the starting point[23].

We recognise that this new approach in the Draft Guidance broadly aligns with the EDPB Guidelines[24] and appears to move the ICO towards harmonisation with EU practices. However, recent decisions by other European supervisory authorities, such as the Irish DPC against TikTok[25], the Italian Garante's decision against Axpo Italia[26], the Spanish AEPD's decision against BBVA[27], as well as the EDPB itself in its decision against TikTok[28], do not follow the proposed calculation in the EDPB Guidelines. None of these decisions (i) apply the distinction between 'the seriousness of the infringement' and 'aggravating or mitigating factors'; nor (ii) calculate a starting point as a percentage of the relevant statutory maximum. Instead, they follow a holistic approach, taking into account all factors under Article 83(1) and (2), before finally checking that the correct statutory maximum is not exceeded.

---

[16] RAP. See page 27.

[17] ICO TikTok MPN.

[18] Clearview AI Inc. monetary penalty notice, issued 26 May 2022 ("**ICO Clearview AI MPN**").

[19] ICO TikTok MPN. See paragraph 206, where the Commissioner *"found that TikTok is likely to have made financial gain as a result of the infringements, but that there is insufficient evidence available to him to calculate the exact amount of the financial gain"*.

[20] ICO Clearview AI MPN. See paragraph 106, where the Commissioner *"[did] not have any figures for Clearview's income, or turnover"*.

[21] ICO TikTok MPN. See paragraphs 261-263.

[22] See paragraphs 109-110 of the Draft Guidance.

[23] See paragraphs 134-135 of the Draft Guidance.

[24] EDPB Guidelines. See paragraph 17.

[25] Decision on DPC Inquiry IN-21-9-1. See paragraphs 307-417, where the DPC (i) considers the factors in Article 83(2) in turn, as part of the Review Stage (see Question 7); (ii) then considers the requirement for the fine to be "effective, proportionate, and dissuasive" as required by Article 83(1); (iii) before finally applying Article 83(3) and checking that the relevant statutory maximum is not exceeded.

[26] GPDP Measure of 28 September 2023 [9940988]. See Section 6, where the Garante (i) first considered Article 83(3) and described the statutory maximums; (ii) then described the requirements under Article 83(1); (iii) before considering the factors in Article 83(2) in no particular order and arriving at the final amount.

[27] AEPD Proceeding No. PS/00677/2022, issued 20 September 2023 (only available in Spanish). See Section VIII.

[28] EDPB Binding Decision 2/2023. See Section 6, where the objections of several other supervisory authorities relating to the administrative fine were dismissed and the EDPB did not raise any concerns regarding the DPC's apparent departure from the EDPB Guidelines when calculating the penalty.

This approach would seem more in line with the UK GDPR itself, which does not suggest any specific order of priority in which the Article 83(2) factors should be assessed, but rather states that due regard should be given to each[29]. This is acknowledged in the EDPB Guidelines[30], the WP29 Guidelines[31], and perhaps best expressed in EDPB Binding Decision 5/2022 which confirms that *"a fine can ultimately only be calculated by weighing up all the elements expressly identified in Article 83(2)(a)–(j) GDPR, relevant to the case and any other relevant elements"*[32].

Further, we are concerned that by calculating the starting point using only a subset of the statutory factors (i.e. Article 83(2)(a), (b) and (g)) this approach would tend to 'overweight' these particular factors when there is no statutory basis for doing so. As paragraph 130 of the Draft Guidance makes clear, the *"adjustment for seriousness"* is **multiplicative** in nature, whereas it is implied that the remaining *"aggravating and mitigating factors"* would only change the starting point on an **additive/subtractive** basis (paragraph 134 of the Draft Guidance).

In light of the above, we believe the ICO's approach in the Clearview AI[33] and TikTok[34] decisions represents a more flexible and practical option that can be developed upon through future decisions.

9. Do you have any comments on our approach to accounting for turnover when calculating the fine?

The ICO notes in the Draft Guidance that the Commissioner may adjust the turnover figure *"by using draft or forecast figures where available"*[35].

We are concerned that relying on forecast figures (particularly if in draft format or gathered from third-party sources) may introduce uncertainty into the penalty Calculation Stage. Forecasts are sensitive to geopolitical and market conditions, economic fluctuations, and changes in company strategic decisions. These can make it challenging for the ICO to accurately determine the exact financial impact of a penalty.

The ICO may wish to consider the possibility of retrospective adjustments to penalties to take account of inaccurate forecasts. This adjustment would ensure that fines accurately reflect financial capacity and do not impose a disproportionate economic burden on controllers[36]. Such a measure would contribute to a fair and equitable enforcement of penalties, fostering greater confidence in the regulatory framework while rectifying any unintended financial burden imposed on businesses.

---

[29] Recital 148, UK GDPR.

[30] EDPB Guidelines. See paragraph 47, which states that *"The identification of harmonised starting points in these Guidelines does not and should not preclude supervisory authorities from assessing each case on its merits."*

[31] WP29 Guidelines. See page 9, which states that *"Article 83 (2) provides a list of criteria the supervisory authorities are expected to use in the assessment both of whether a fine should be imposed and of the amount of the fine. This does not recommend a repeated assessment of the same criteria, but an assessment that takes into account all the circumstances of each individual case, as provided by article 83. The conclusions reached in the first stage of the assessment may be used in the second part concerning the amount of the fine, thereby avoiding the need to assess using the same criteria twice."*

[32] EDPB Binding Decision 5/2022. See paragraph 313.

[33] ICO Clearview AI MPN.

[34] ICO TikTok MPN.

[35] See paragraph 123 of the Draft Guidance.

[36] Section 108 Deregulation Act 2015.

10. Do you have any comments on how we apply aggravating and mitigating factors when calculating the fine?

In applying the factors under Article 83(2)[37] for both the Review and Calculation Stages, we would invite the ICO to consider the following:

Factors should not be predetermined as either 'aggravating' or 'mitigating'

The UK GDPR does not explicitly designate which of the Article 83(2) factors are aggravating or mitigating. Instead, it is understood that, when considering whether to impose a fine, the Article 83(2) factors are applied together and as a whole, turning on the facts of each individual case (as noted in Question 7 and 8 above)[38].

Whilst we welcome the practical examples illustrating the ICO's interpretation of Article 83(2) in the Draft Guidance, we would ask that the ICO considers each factor from a neutral starting point, and avoids suggesting upfront whether certain factors would have a primarily 'aggravating' or 'mitigating' effect (thus only either increasing or decreasing the fine, accordingly), without regard to the specific context.

This approach would preserve the inherent flexibility of the UK GDPR assessment, and along with Article 83(2)(k), which is already fact-specific in nature, would allow the ICO to adapt to new and evolving sectors with unique business circumstances.

Assessment of remedial action

We would also welcome further guidance in relation to how the ICO assesses remediation steps taken by controllers, in particular remediation steps taken prior to any investigation action by the ICO.

The WP29 Guidelines note that timely remedial action to stop an infringement from continuing is accounted for when considering actions to mitigate the damage suffered by data subjects under Article 83(2)(c)[39]. Recent EU decisions have also considered proactive steps taken by controllers / processors to end to an infringement as mitigating under Article 83(2)(a), (c), and (f) holistically[40].

However, the Draft Guidance does not seem to address the ICO's position regarding the mere cessation of an infringement, neither in paragraphs 86-89, which focus on assessing the degree of cooperation under Article 83(2)(f), nor paragraphs 74-76, which focus on mitigation measures to alleviate damage suffered by data subjects under Article 83(2)(c). Paragraph 76 of the Draft Guidance specifically notes that the Commissioner is likely to give less weight to "*actions that have **no effect** (or only a limited effect) on **mitigating the damage suffered** by the data subjects*" (emphasis added).

We are conscious that by failing to explicitly mention proactive remedial actions to end an infringement, along with the deprioritisation in paragraph 76 of actions that do not mitigate the harm suffered by data subjects, the Draft Guidance risks discouraging controllers from considering proactive steps which, whilst they may not necessarily repair or compensate for damage already caused to individuals, they may, for example, (i) stop the infringement from continuing to cause additional harm; and / or (ii) prevent the infringement from causing harm to other data subjects in the future.

---

[37] We have proceeded on the basis that footnotes 68, 71, 73, 75, and 77 in the Draft Guidance are intended to be references to Article 83(2).

[38] This is also highlighted in the WP29 Guidelines. See page 7, which states that "*the Regulation requires assessment of each case individually*".

[39] WP29 Guidelines. See page 13, which states "*timely action taken by the data controller/processor to stop the infringement from continuing or expanding to a level or phase which would have had a far more serious impact than it did*" is considered under Article 83(2)(c).

[40] For example, Decision on DPC Inquiry IN-21-9-1. See paragraphs 342-360, where the DPC considered remediation measures taken by TikTok under Article 83(2)(a), (c), and (f).

We recognise that this is unlikely to be the ICO's intention[41]. As such, we would invite the ICO to: (i) comment on how remedial actions and infringements already cured are factored into the ICO's assessment (whether under 83(2)(c), 83(2)(f), 83(2)(k), or holistically), particularly where remedial actions took place prior to any investigative action by the ICO; and (ii) clarify its approach in the Draft Guidance.

11. Do you have any comments on how we make any necessary adjustments to ensure the fine is effective, proportionate and dissuasive?

We recognise and agree that Article 83(1) requires any fine imposed to be "*effective, proportionate and dissuasive*". However, paragraphs 144-146 of the Draft Guidance appear to suggest a specific order in which these concepts will be considered: (i) effectiveness; **then** (ii) dissuasiveness; and **finally** (iii) whether the fine is proportionate.

We understand that the ICO has applied a similar order in previous decisions (e.g. TikTok[42]), but this approach is not reflected in the EDPB Guidelines, nor does it appear to have been explicitly adopted by the EDPB or other EU supervisory authorities. We would therefore welcome clarification from the ICO as to why this particular order has been chosen.

12. Do you have any other comments on our five-step approach to the calculation of the appropriate amount of a fine?

No further comments.

[41] We note that the ICO considered remedial actions in its recent ICO TikTok MPN. See paragraphs 234 and 235.

[42] ICO TikTok MPN. See paragraphs 253-257.

Financial hardship

13. Do you have any comments on our approach to financial hardship?

No comments.

Any other comments

14. Do you have any other comments on the draft Data Protection Fining Guidance?

We strongly support the ICO's efforts to provide organisations operating within the UK's data protection framework with clarity on the ICO's risk-based approach to regulatory action and we are grateful for the chance to respond to the ICO's consultation on its Draft Guidance.

In addition to our above submissions, we would welcome clarity on the implementation timeline, and whether the ICO intends to apply the Draft Guidance, once finalised: (i) on a 'look-forward' basis only (i.e. to issues arising only after the effective date of the Draft Guidance); or (ii) retrospectively (i.e. to all current and past matters it investigates under UK law, from the date the Draft Guidance becomes effective).

Thank you for the opportunity to comment on this important matter.