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:

[redacted] Apple Distribution International Ltd.

We discussed the consultation [redacted]

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?

We appreciate the clarity this section brings, in particular the explanation of why EU concepts and definitions will continue to apply in the UK. We are somewhat surprised that this is an area where the UK intends to remain so closely aligned to the EU, particularly given the strategic priorities proposed for the future Information Commission, and industry critique on the application of the EU concept of undertaking to the GDPR.

There are reasonable concerns from industry about transposing definitions developed in years of competition case law to data protection matters that in our view do not share the same legal qualifiers. Often competition cases involved deliberate highly profitable infringements such as cartel formation, for which penalties should rightly be steep and entities should not be able to hide behind corporate structures. We would argue that does not directly translate to a data protection regime, which regulates the conduct of controllers and processors in their processing operations and not of undertakings generally. Competition law has no equivalent of controller or processor as responsible entities and has no concept of relevant processing activities undertaken by any such entities. As such, there is a sound argument that competition law principles and concepts (e.g. the single economic entity concept) should not generally be applied in the context of GDPR administrative fines. When calculating the maximum fine under the GDPR, the turnover should be that of the infringing controller/processor, rather than their parent company.

The two regimes have developed to protect against very different harms, as shown by the fact Articles 101 and 102 are only mentioned in a single GDPR recital. It would therefore be concerning if this single reference in a recital were to be taken as the basis to impose competition law principles generally on the very different regime set out in the GDPR.

Further we are aware that the question of whether EU data protection authorities should in fact be using the definition from competition law is currently with the CJEU and could lead to a divergence in the ICO's approach.

We appreciate the draft guidance sets out a rebuttable presumption for subsidiaries to challenge whether their parent company exercises influence over them. However, the starting position that the parent exercises control simply because it holds all shares is a very steep bar in practice as demonstrated by recent EDPB decisions. Being a shareholder does not in and of itself mean the parent has any say in the data decisions taken by its subsidiaries, which must be the focus of any UK GDPR infringement investigation. The concept of "decisive influence" of a parent over a group company in the data protection sphere can only relate to the issue of the processing of personal data and not to influence of a parent over its subsidiary in some other undefined aspects.

In the case of global companies such as Apple, taking the starting point of the ultimate parent company for the actions of its European subsidiary, who is the responsible entity for taking decisions about data of users in Europe, would be disproportionate and difficult to align with natural justice principles.

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

We welcome the clarity and brevity of this section and note it compares favourably with the equivalent section in the relevant EPDB guidance. We feel it would be helpful to separate out and expand upon each example so that the reader can more easily see the outcome for each scenario. This could involve setting out the total maximum fine the company could face for the 'same or linked' and separate conduct examples.

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

No.

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?

We again appreciate the efforts taken in setting out your approach clearly. It is helpful, although not a straightforward task, to outline general principles when decisions will be fact-specific. We feel the guidance could benefit from it being clarified that not all factors would be present in all cases and that the ICO would make a thorough case-by-case assessment.

The section also reads like it would be very hard for a company of the scale and sector of operation of ADI to avoid a finding that any infringement is serious. By their nature any potential infringement could involve innovative technologies, be conducted at a large scale, be central to ADI's business model and therefore be serious, even if the potential harm to individuals was minor.

We feel that the guidance should clarify that any intentional infringements that were profitable for the controller should be considered the most serious, whereas unintentional or technical infringements that led to little or no harm should not be qualified as serious simply because of the number of affected users where the potential harm itself remains

negligible under the law. Although this is discussed as an aggravating factor, we feel it goes to the heart of the seriousness assessment. This is particular important given the effect of the seriousness determination in the draft guidance. It would be counter to the intention to encourage all data controllers to take serious steps to mitigate risk under data protection law, to potentially set any such mitigations to nought where a data controller is of a certain size operating in a particular sector.

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

It is again helpful to have a thorough indication of the approach the ICO will take in general whilst noting it will be a case-by-case assessment.

The impression the guidance gives as drafted is that your office will view most factors as aggravating or neutral, and that it will be quite hard in practice to meet the mitigation standards. We feel this may be unintentional as there should be positive incentives for data controllers to invest in data protection. Where a data controller does so and suffers an unintentional breach there should be an ability to highlight genuine mitigation attempts.

Whilst of course expected of controllers to comply with the UK GDPR, we suspect the ICO has discovered that compliance standards vary, and that certain companies take additional measures to go beyond the legal minimum and adhere to higher standards of privacy because that is the right thing to do. We therefore think special efforts to advance privacy by design principles, sound internal record keeping and avantgarde technical and organisational measures such as those utilised at ADI should be given weight as significant factors in a scenario where other organisations with a simpler compliance approach would have experienced stronger privacy impacts. Likewise, cooperation with your Office must vary significantly, so the positive approach taken by companies such as ADI should be taken into account as assisting any investigation. This is particularly true where the rebuttable presumption is in play and the parent company may take a different approach.

We believe that an international company such as ADI should not be penalised for not raising any potential infringements with your Office as a primary contact point. Considering that our lead supervisory authority under the GDPR one stop shop is the Data Protection Commission in Ireland, were we to suffer a Europe-wide incident we would likely be liaising primarily with the DPC and feel this should not be considered negative. Whilst we would of course aim to inform any supervisory authorities in countries affected by the incident, it should be recognised that it is not practically possible to engage with all given the evolving nature of security incidents. Requiring ADI to adopt a simultaneous approach in the face of a time sensitive event and differing queries from

multiple authorities may in fact detract our attention from mitigation efforts. This is not to say that ADI would waive its responsibility of exchanging with and informing your Office accordingly. To the contrary, ADI has and intends to maintain a positive collaborative relationship with the ICO. Therefore, in view of the strong international cooperation between your office and EU DPAs, we would kindly ask that the penalisation discussed above be reconsidered.

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

This section is also clear.

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 were pleased the guidance specifically states that it will not be always appropriate for the ICO to levy a penalty notice. The ICO is known for being pragmatic and we generally agree with its approach of educating, engaging and encouraging before enforcing. There is potentially an opportunity to make this prominent approach clearer in the draft guidance itself.

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?

As we set out above, we feel that if your Office were to assess seriousness strictly by the terms of the guidance, this would lead to relatively minor harms being judged as serious without a clear rationale for doing so in certain cases. Such strict application of the guidance would have significant negative consequences for ADI as the starting point would be a proportion of a large turnover, which appears to be weighted more importantly than the actual privacy outcomes for the affected individuals. We believe that factors such as the intentional nature of the infringement and any financial benefit obtained as a result of the infringement should be given more weight at this early stage.

Furthermore, the guidance as written could be clearer in explaining the logic behind the banding. Using categories of Low, Medium and High would imply three equal levels, so starting percentages could be roughly evenly spread.

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

Whilst we understand the need for fines to be effective, proportionate and dissuasive, we feel using such a formulation would lead to ADI being potentially liable for large fines simply due to the size of the organisation or its parent. For the reasons set out above, if the ICO were to follow the terms of the guidance as is, it would be able to class a low-level incident as serious due to ADI's scale even where no real harm arises from the event. This would mean a possible fine of 4% of Apple Inc's turnover, which would not be adjusted. Mitigating factors as currently drafted would not seem to reduce the starting point by much. This would mean a fine in the multiple billions of pounds for an event that would not have a real impact on the privacy of the individuals, a fine which would also lack a deterrent effect due to the absence of an actual gap in compliance.

We do however note these are indications only and the Commissioner will take a case-by-case decision. We also appreciated the clear worked examples. We also note that the equivalent EDPB bands overlap, allowing for more flexibility in calculating the starting point.

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

No.

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

We note the Commissioner retains a large degree of discretion to adjust the fine significantly. Whilst this somewhat undoes the predictability of the earlier tables, we agree with the approach. Fining decisions will need to take all relevant considerations into account and should not follow a deterministic method.

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

No.

Financial hardship

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

No.

Any other comments

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

No.