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:

Our organisation is called Aria Grace Law CIC. This consultation has been populated by [redacted]

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

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):

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?

No comments.

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

We think it would be helpful for the ICO to provide more information and examples on "linked" conduct because it could be argued that all processing operations could be "linked" due to how organisations operate and the data protection principles that need to be applied by an organisation across it. Where there are separate infringements arising from separate conduct for the same organisation, we think it would be helpful to have more information on the ICO's approach. This is because from paragraph 45, we understand that each infringement would be subject to the relevant statutory maximum with the total amount exceeding the amount specified for the gravest infringement. As the total penalty amount could be extremely high, it would be useful to understand more about the ICO's approach when it concerns separate infringements arising from separate conduct and how it determines when an infringement is really separate conduct and not "linked" conduct.

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

No comments.

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 think it would be helpful for the ICO to consider explicitly referring to and giving examples of the different categories of data subjects affected (rather than only the categories of personal data affected). This is because certain data subjects are more vulnerable.

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

We think it's helpful that the ICO will be taking into account the size and resources of an organisation and also the nature and purpose of the processing. It would be helpful if the ICO provided more information on the topic of "resources" and whether its referring to funds, employees, contractors, systems etc. (or all of them).

If the ICO is referring to employees, would it consider if an organisation could not afford a dedicated employee for IT purposes (to cover security)?

In addition, would the ICO penalise an organisation if it was required to put in place a Data Protection Officer but failed to do so as it did not have the resources to do so?

We have seen organisations that are in principle committed to complying with data protection law; however, due to the accountability principle and the number of requirements under the law, such organisations are not able to comply fully in practice due to limited resources.

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

The ICO has stated that in paragraph 91 that if an organisation has brought a violation to its attention then, the ICO may consider this as a mitigating factor.

In paragraph 92, the ICO has stated that paragraph 91 would not be applicable, if the organisation is required to inform the ICO due to the organisations' statutory obligations. We think it would be helpful for the ICO to state examples in paragraph 91 as to when an organisation would engage with the ICO voluntarily about a violation (except for when required to do so under statue). This is because we believe that organisations would find it helpful to know when the ICO would expect them (outside of their statutory obligations) to communicate with the ICO in respect of a violation.

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 think it would be helpful for the ICO to consider explicitly referring to and giving examples of the different categories of data subjects affected (rather than only the categories of personal data affected).

We think it would be useful for the ICO to incorporate examples of its previous enforcement action and where it has identified aggravated and mitigating factors. This is because it will help organisations to see real-life examples of how the ICO determines aggravated and mitigating factors.

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?

No comments.

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

No comments.

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

No comments.

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

No comments.

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

Our experience of the ICO is that it is very good at presenting information. In respect of the calculation section of the guidance, we feel that it would be helpful, however, if the ICO created a more user-friendly summary for smaller organisations as they may struggle to understand the detail in the five-step approach.

Financial hardship

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

We think it would be useful if the ICO could provide more information on the types of payment plans that it could enter into with organisations where their application for financial hardship is accepted. Some organisations which are struggling financially may not have the commercial acumen and/or resources to come up with a payment plan. It may be helpful if the ICO provides examples of payment plans that it has entered into in the past and how they have worked (e.g., £X due in month one, £X amount due in month two, £X amount due in month three etc.). Some small organisation especially start-ups have cash-flow issues and we think they would benefit from greater insight in respect of the payment plans in the event that they receive a penalty notice from the ICO.

Any other comments

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

We found it to be very useful and informative. While the Regulatory Action Policy was a great basis in understanding of the ICO operates in respect of investigations and enforcement, the Data Protection Fining Guidance is certainly welcome due to the amount of detail included.