Consultation questions: Data Protection Fining Guidance

Start date: 2 October 2023

End date: 27 November 2023

About you

Your name:

██████████████

Email address:

███████████████████████

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:

Lloyds Banking Group

████████████████████████

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?

As there is no clear definition of undertaking in the context of fines – visual representation would be useful. Detailed examples of how the ICO are planning to enforce the definition of an undertaking in relation to fines would also be useful.

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

A breakdown of how this would be considered would be helpful. There is mention that seriousness will be considered, but where there are varied levels of seriousness, an example would better explain the considerations.

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

More examples would also be useful.

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?

Clear definition with examples of what would amount to a low, medium and high level of seriousness would be useful here.

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

Detailed examples would be useful here, if possible – a clearer understanding of how aggravating or mitigating factors may impact the final fine amount.

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

More examples would be useful here also.

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'?

More examples here also – full end to end (decision tree could be useful).

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?

More detailed examples would be useful here also.

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

More examples would be useful here also.

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

See answer to Q5.

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

More examples would be useful here including definition of effective, proportionate, and dissuasive in this context.

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

Guidance is very vague in relation to the five-step approach. More examples would be useful in supporting a stronger understanding. Especially in relation to the assessment, it is unclear as to what constitutes a high, medium, and low degree of seriousness.

Financial hardship

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

"Financial hardship" – will this be calculated and broken down at industry level i.e., public sector vs private? How will this be done in a way that doesn't cause bias? More guidance regarding approach required. Examples of what would be a sufficient hardship to be considered would be useful.

Any other comments

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

Overall, the guidance is helpful, but each area could use more examples, and some areas could specifically do with lower-level breakdowns.

"The manner in which the infringement became known to the Commissioner" – more explanation would be useful here, especially regarding what is considered to be "neutral" (para 93) when infringement is notified to the ICO by anyone other than the Controller or Processor. More clarity on what would amount to a good/neutral/bad aggravating factor would be great.

As an aside, we recognise that it's challenging to provide very prescriptive guidelines on how fines are calculated, as bad actors may use this to justify bad faith risk-based decisions, i.e. 'we stand to gain £1,000,000, and the max we could be fined is £100,000, so we should proceed with this activity'. That said, the more information that can be provided, the more easily Privacy experts in good actor organisations can highlight the seriousness and importance of following Data Protection legislation. We would welcome any amount of further clarity and detail you're able to provide.