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:

Lucid Privacy Group

[redacted]

Views have been obtained by open discussion and debate after a close reading of the guidance

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?

-

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

-

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

-

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?

-

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

-

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

-

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'?

-

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?

-

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

-

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

-

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

-

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

-

Financial hardship

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

-

Any other comments

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

We are generally supportive of the guidance. We anticipate that many of our clients will be relieved to see a strong degree of continued harmonization with the similar guidance issued last year by the EDPB. International businesses that have both EU and UK GDPR obligations in both jurisdictions generally will tend to favour harmonisation to reduce the complexity and cost of managing a divergent privacy programme. In analysing how to efficiently and effectively develop a privacy programme and to resource it properly, having an understanding of potential regulatory losses is an important input factor that organisations will typically analyse. Added complexity to this side of the analysis would be a challenge.

That said, there will of course be organisations, especially those with no EU GDPR obligations (UK national orgs or international orgs with UK presence but no EU presence) who may have been hoping for a softening in this area. There is already an in market perception that the ICO is more business friendly as a regulator than some European counterparts, and as such there could have been an opportunity to diverge (within the confines of the UK GDPR) on fine calculations as an issue of UK competitive advantage.

These are interesting issues that speak to the fact that the interplay here between UK and EU jurisdictions is a central issue for how organisations will be thinking about this guidance. With that in mind we would have expected the guidance to perhaps touch on this issue. As an example, clarification on 'double jeopardy' type scenarios in which organisations post-brexit find themselves at risk of multiple enforcement actions in both jurisdictions would be welcome. Would proportionality come in to play if an organisation is facing enforcement

action on both sides? Some brief guidance on this issue would be very useful.

The other comment we would like to make here is on the interplay with UK legislative change. This methodology is of course based on the UK GDPR, which is likely to be replaced in the coming year(s). How long will this guidance be valid for post-publication? Will this guidance have merit in the new UK data protection regime? This information would be essential for organizations planning their medium term compliance strategies.