Consultation questions: Data Protection Fining Guidance

Start date: 2 October 2023

End date: 27 November 2023

About you

Your name:

Jay Libove

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:

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

Professional

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):

I consent

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?

There is no need for actual harm to have occurred, in order for penalties to sometimes be appropriate.

Negligence which went on despite notification by a consumer, civil society group, or anyone at all, must cause the ICO to consider the act to become intentional, even though it began as negligent.

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

Negligence that went on despite notice by a consumer, civil society group, or anyone at all, must aggravate the assessment of the seriousness of the violation.

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?

I filed a complaint to the ICO about a material non-compliance by a financial services company (an implementation of required-by-regulation 2-factor authentication that was trivially bypassable) and which the responsible company persisted for six months in insisting that the already-well-demonstrated vulnerability did not exist. I notified that company via its customer care function, it's report-a-security-vulnerability function, directly to a security management employee through my professional network, then finally to the company's head of risk. I also advised a journalist of the issue, and the journalist used a personal-professional contact at the company. Only after the head of risk contact and/or the journalist's contact did the company finally acknowledge the amply demonstrated, trivially executed security bypass, and fix it. The ICO took the position that "no proven harm had been done" and "company had fixed it" and chose to NOT impose a penalty. Clearly, the ICO's process failed to properly assess the negligent-became-intentional nature, incorrectly relied on "no proven harm done", and missed a great opportunity through either/both a notice to correct or a notice of enforcement to put on notice all other actors that "when we say you must have adequate security controls, we mean it". I was supremely disappointed in the ICO's lack of concern and lack of action, and I hope that this current process results in an ICO that properly penalizes on-going negligent-becoming-intentional bad behavior, and does not in future fail to use its voice to prevent other companies continuing the status quo of "until we get caught and punished hard we'll assume that cheating is cheaper than complying".