Consultation questions: Data Protection Fining Guidance

Start date: 2 October 2023

End date: 27 November 2023

About you

Your name:

Keller Postman

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:

Keller Postman

[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?

A: This approach should incentivise large corporations to adhere to regulatory standards across the entirety of their portfolio, as the risk of one subsidiary falling short of standards would be applicable to all. This approach would address public concerns that large companies have been able to offset penalties or receive lighter reprimands by sacrificing subsidiaries to minimise the impact of ICO rulings.

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

A: The proposed approach to fines where there is more than one infringement by an organisation broadens the scope of Article 83 (3) GDPR (General Data Protection Regulation) which ultimately imposes a limit on the maximum fine amount: 'the overall fine imposed by the Commissioner in relation to infringements arising from those processing operations must not exceed the maximum statutory amount that applies to the most serious of the individual infringements identified.

This approach streamlines the process, ensuring that 'each infringement would be subject to the relevant subject statutory largest amount. Other than to consider the proportionality requirement, the combined penalty amount for each infringement 'may exceed the amount specified for the gravest infringement.

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

A: Overall, the proposed changes are welcome. Procedures found in RAP (Regulatory Action Policy) have been bolstered in the DPFG (Data Protecting Fining Guidance), streamlining rules, procedures, and balancing proper punishment with proportionality.

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?

A: It will be difficult to accurately define 1.1 and 1.2 in some cases. Often hard to prove whether an action is intentional or negligent. Nature and duration can be quantified, gravity can be less readily quantified - will the ICO assess 'actual' harm for example or 'potential' harm?

Why not include the number of data subjects affected?

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

A: Section 76 of the DPFG states that if the action taken by the processor or the controller 'had no effect (or only a limited effect)' on the damaged suffered by the victim of the breach, that the Commissioner will give it less weight.

Whilst the rationale of this approach is sound. It does not recognise that factors beyond the control of a processor or controller that to varying degrees could limit the effectiveness of the efforts made to mitigate any damage.

It would be more balanced to ask that controllers or processors show the action taken to mitigate any breach. This should then be compared to an ICO issued policy on mitigating action. If it can be proved that the accused followed ICO policy, in addition to their own procedures, took the best possible approach to tackle the breach, but that factors beyond their control hindered the effectiveness of their action, then the commissioner should view this favourably, or at least not take less 'weight' from the accused actions.

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

A: The proposed approach supplies clarity on the above criteria which allows the accused to, in theory and looking through a non-bias-eye, broadly estimate the penalty that they might receive. Should there be a noticeable difference in penalty between what was expected and what was issued (which should have been decided using the three above

assessment criteria, would open the opportunity for a successful appeal, a lengthy and costly process for the accused and accuser.

We welcome Section 105 of the DPFG which highlights the Commissioners obligation under section 108 of the Deregulation Act 2015 which says that 'the Commissioner will have regard to the desirability of promoting economic growth'.

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'?

A: The approach seems reasonable and appears to consider the relevant criteria. I do believe fines should be considered a last resort after reprimands and ordering compliance.

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?

A: Starting point is reasonable. We welcome that no pre-set 'tariff' starting points for fines have been introduced.

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

A: Turnover and revenue are not necessarily and indicator of healthy finances. This approach raises proportionately issue for parent companies.

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

A: The approach seems reasonable though for large corporates it will always be difficult to meet the third criteria i.e., dissuasive, as in many cases the fine will not be greater than the company's potential

commercial advantage from non-compliance (e.g., social media companies).

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

A: The approach seems reasonable though for large corporates it will always be difficult to meet the third criteria i.e., dissuasive, as in many cases the fine will not be greater than the company's potential commercial advantage from non-compliance (e.g., social media companies).

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

A: The revised approach seems balanced.

Financial hardship

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

A: We would like the ICO to supply further clarification on Financial Hardship application and assessment process.

Complications may arise for parent / subsidiary organisations…Could a subsidiary organisation submit a claim for Financial Hardship if their parent company is in a sound financial position? If no, to what extent would the parent company be liable? Would a formula need to be developed which considered extent of influence over subsidiary entities before deciding liability?

Any other comments

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