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:

Handley Gill Limited

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

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

At para.41 it is stated that *"Where the Commissioner finds that a controller or processor's overall conduct has infringed more than one provision of the UK GDPR or Part 3 or Part 4 DPA 2018, the Commissioner will apply Article 83(3) UK GDPR and identify the statutory maximum applicable to the most serious individual infringement"*. The Commissioner cannot apply Article 83(3) UK GDPR to Parts 3 and/or 4 DPA 2018, albeit that it can apply the same principles and/or act consistently with it.

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

We note that at para. 10 it is stated that *"This fining guidance applies from the date of publication to new cases relating to infringements of the UK GDPR or DPA 2018. It also applies to ongoing cases in which the Commissioner has not yet issued a notice of intent to impose a fine"*. We consider that to apply the new guidance to incidents which occurred prior to its publication in circumstances where this would serve to impose a greater penalty or other adverse impact would involve the inappropriate imposition of a retrospective penalty which could violate Article 1 of Protocol 1 of the European Convention on Human Rights and infringe the principle of regulatory certainty.

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?

While we note and acknowledge the relevance of the information Commissioner considering the nature of processing, including whether the activities might be deemed 'high risk' in which case additional weight may be given to this factor, we consider that the Information Commissioner also ought to give consideration to whether the nature of processing is such that it is in the public interest or otherwise in the exercise of fundamental rights, for example in relation to processing for the special purposes or for the purposes of the prevention or detection of crime by competent authorities, which could act as a countervailing factor.

The factors to be addressed appear to involve duplication, for example the number of affected data subjects is stated to be relevant to both the scope of the processing and the number of data subjects affected, which could result in undue weight being afforded to certain factors if the assessment of each is undertaken in isolation rathe

In relation to the purpose of the processing, similarly to our position in relation to the nature of processing, we consider that the Information Commissioner also ought to give consideration to whether the nature of processing is such that it is in the public interest or otherwise in the exercise of fundamental rights.

We would appreciate further clarity as to how the purpose of processing factor would be applied in practice, and consider that the current wording again duplicates considerations relevant to other factors.

In relation to the level of damage suffered, in so far as reputational harm may be a relevant consideration, we consider that this should only be taken into account in connection with unwarranted reputational harm.

The draft guidance states that *"some harms are more readily identifiable (for example, financial loss or identity theft) whereas others are less tangible (for example, distress and anxiety or loss of control over personal data)"*. It is not clear whether the English courts would acknowledge that loss of control over personal data in and of itself constitutes a legitimate harm for the purposes of the UK GDPR and/or Data Protection Act 2018 (see Lloyd v Google LLC [2021] UKSC 50).

In relation to the assessment of negligence it is stated that *"infringing UK GDPR or DPA 2018 through human error, particularly where the person (or people) involved had not received adequate training on data protection risks"*. We do not consider that human error in and of itself is necessarily indicative of negligence; we do accept that human error coupled with a lack of training or inadequate procedures to provide for safeguards would be capable of constituting negligence. In the same section, we do not consider that *"failing to check for personal data in information that is published or otherwise disclosed"* is itself evidence of negligence, but that a failure to have in place policies and procedures, staff training and an approval mechanism to ensure that personal data is identified and removed prior to publication or disclosure would constitute evidence of negligence.

At para.72 it is stated that *"In assessing seriousness, the Commissioner may also take into account other types of personal data affected by the infringement where that data may be regarded as particularly sensitive. This includes where the dissemination of the personal data is likely to cause damage or distress to data subjects, for example: location data…"*. We do not consider location data, in and of itself, will necessarily be likely to cause damage or distress to data subjects and note in this regard that the Information Commissioner's 'Overview of Data Protection Harms and the ICO's Taxonomy' (April 2022) does not suggest otherwise.

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

At para.81 it is stated that *"In the light of the level of accountability expected of controllers and processors under UK GDPR and Part 3 and Part 4 DPA 2018, it is more likely that the Commissioner will consider the degree of responsibility to be an aggravating factor or, at best, a neutral factor. In order for this to be considered a mitigating factor, a controller or processor will need to show that it has gone over and above its obligations under UK GDPR and DPA 2018."* We do not consider that a requirement to exceed legal obligations is a necessary or legitimate precursor to determining degree of responsibility, which would otherwise render the provision otiose.

At para.98, non-compliance with an approved code of conduct or certification mechanism are stated to constitute evidence of intentional or negligent conduct, but these factors are not stated as being relevant to the consideration of intentional or negligent conduct in relation to the seriousness of the infringement and could again result in certain factors being double counted and therefore afforded undue weight.

At para.100, we anticipate that, in addition to recognising the NCSC, it would be appropriate to recognise reporting to the police and (where appropriate) Action Fraud as appropriate authorities.

We would query whether it would be appropriate here to recognise that, in accordance with the Information Commissioner's stated policy, payment of a ransom will not be considered a mitigating factor.

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

We welcome the Information Commissioner's recognition that a failure to enforce data protection law has anti-competitive consequences and has a dissuasive impact on compliance.

We would welcome inclusion in the guidance of indicative factors that will be taken into account in considering proportionality.

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?

The indication that the starting point for the *"most serious infringements"* will range from 20-100% of the available maximum without further guidance lacks clarity and fails to provide regulatory certainty.

We consider that the lower and medium levels of seriousness could attract more significant upper limits and that level of overlap between the bands for the various levels of seriousness may be appropriate. This is particularly so given that the Information Commissioner would already have considered that an administrative penalty is appropriate in addition to or instead of one of its lesser interventions.

It is perhaps surprising that the Information Commissioner considers, as stated at para.114, that an incident deemed to be within the *"most serious category"* which does not attract mitigating or aggravating factors would be limited to 40% of the maximum, subject to reduction due to the size of the undertaking for example. The impact is demonstrated at Tables C and D, which indicate that in many cases an administrative penalty will not be levied even where it was originally considered appropriate and that is even before any mitigating factors are taken into account and that the guidance thereby fails to meet the requirements that penalties be effective, proportionate and dissuasive. We consider that the Information Commissioner ought not to fetter its discretion as will inevitably be the case by virtue of this guidance.

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

While we note that Information Commissioner's approach in considering the undertaking's worldwide annual turnover in the previous financial year, which we understand to mean in the financial year immediately preceding the Information Commissioner's consideration of the fine, we would query whether the worldwide annual turnover in the year of the relevant infringement (or an average of the turnover in the relevant years of the duration of the infringement) would be more appropriate, which would also ensure that any delay in enforcement did not adversely affect the relevant undertaking or have a disproportionate impact taking into account the to the obligation to have regard to the desirability of promoting economic growth, as required under section 108 of the Deregulation Act 2015.

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

We would welcome the inclusion of indicative mitigating and aggravating factors, including reference to the Information Commissioner's guidance on the payment of a ransom.

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

We welcome recognition that there will be cases, such as where an undertaking's core business is reliant on the sufficiently serious unlawful processing of personal data at scale, where the imposition of administrative penalty of such an amount that the undertaking would be rendered insolvent is both appropriate and necessary.

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

No

Financial hardship

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

We welcome recognition that payment of an administrative penalty by instalments is preferable to forcing an undertaking into insolvency and thus depriving the public purse while enabling the relevant shareholders and directors to retain the benefit of the unlawful conduct.

Any other comments

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

No