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:

National AIDS Trust

[redacted]

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 specific comments.

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

No specific comments.

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

We welcome the information contained in the section on 'Statutory Background'. It clearly sets out the situations where the Commissioner can impose a fine, the factors that will be taken into account when imposing a fine and the maximum amounts that can be fined. We think that this section would be useful in our advocacy supporting people living with HIV who have experienced breaches of their personal health data such as their HIV status.

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?

We agree with the guidance as written sets out sensible guidelines for assessing the seriousness of an infringement. We would however argue that there should be an additional criterion for assessing the level of damage suffered as a result of a data breach: whether equalities or human rights legislation has potentially been breached. This is because some data breaches can occur because of discriminatory intent, or alongside breaches of human rights.

For example, the most common kind of discrimination experienced by people living with HIV is when their HIV status is shared without their consent. This happens in a number of settings, including in employment, in healthcare, by the police and from acquaintances in their personal life.

These incidents fall under the definition of personal data breaches of special category data. Many of these breaches occur either because of a mistaken belief that such a data breach is necessary to safeguard others health or to prevent HIV transmission. However, some of these breaches of confidentiality of an individual's HIV status are driven by malice from the stigma surrounding HIV, and amount to discrimination under the Equality Act 2010 or breaches of human rights under the Human Rights Act 1998. National AIDS Trust have dealt with over 20 such cases in the last year alone.

Therefore, we believe that a criterion should be whether there has been a potential breach of equalities and/or human rights legislation as part of scrutinising the level of damage suffered when assessing the

seriousness of an infringement. We think doing so will allow the ICO to fulfil its Public Sector Equality Duty under the Equality Act to eliminate discrimination against people living with HIV.

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

We think this approach to assessing relevant aggravating and mitigating factors seems sensible.

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

We think this approach to assessing whether imposing a fine is effective, proportionate and dissuasive seems sensible.

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'?

No specific comments.

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?

No specific comments.

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

No specific comments.

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

No specific comments.

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

No specific comments.

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

No specific comments.

Financial hardship

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

No specific comments.

Any other comments

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

National AIDS Trust welcomes the publication of this draft Data Protection Fining Guidance. When supporting people living with HIV who have experienced breaches of confidentiality related to their HIV status, we have often found it difficult to understand how the ICO assess how and when fines are issued in relation to data protection breaches. We believe this guidance will be helpful in our work supporting people living with HIV who have their special category personal data breached.