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:

The British Insurance Brokers' Association (BIBA) is the UK's leading general insurance intermediary organisation representing the interests of insurance brokers, intermediaries and their customers. BIBA membership includes around 1,800 regulated firms, employing more than 100,000 people. BIBA is the voice of the broking sector advising members, Government, consumer bodies and other stakeholders on key insurance issues.

[redacted]

BIBA has a dedicated Cyber Committee of member brokers and (re)insurance providers to help inform us on key cyber/financial resilience matters in insurance distribution and the regulatory environment.

BIBA calls :

We would like to draw attention to 'Cyber Insurance as a Service' and its role supporting cyber resilience and data security alongside other mitigating measures.

We would like to understand the accountability of software providers and managed service providers when determining outcomes.

It would be helpful to understand the use of precedent by the ICO in coming to decisions.

Would a single 'appropriate body' help businesses and law enforcement connect at a very stressful time?

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):

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?

BIBA Response:

(i) Does the ICO consider investment in comprehensive cyber insurance to be another mitigating factor for the prevention and resolution of data breaches from cyber incidents?

Insurer response teams aim to provide immediate resource and expertise to minimise the impact of cyber incident and data breach. This may include cyber security engineers and forensic specialists to advise on how to make safe a breach, and communications resources to contact customers and legal advice.

Cyber Insurance as a Service includes 24/7 threat monitoring and vulnerability scanning. These extra steps may help prevent a cyber attack and avoid a data breach.

(ii) Where 3rd party software is the cause of a cyber related breach, or a zero-day attack/vulnerability occurs, how does the ICO take this into account? Assuming an organisation has taken reasonable measures to secure its data.

(iii) Where an organisation (e.g. SME) trusts it's IT operations and security to a managed service provider, and that provider fails, to what extent does the ICO consider this to be a mitigating factor?

Some organisations may claim; "how can I know what I do not know" when considering technical and organisational measures they trust to other professionals.

(iv) There may be some organisations that aren't fully aware of, or have previous reason to engage with bodies such as the NCSC. How would the ICO bring these to the attention of organisations and businesses to help?

(v) We agree that a controller or processor following a breach may consider engaging with an appropriate body, such as the NCSC, NCA, Action Fraud, FCA. Would the ICO also give consideration to when in the midst of a malicious cyber incident, reporting to multiple authorities requires resource and direction that may not be the cyber victim's immediate priority. Would a single appropriate body be helpful? They could cascade the information to other such bodies.

(vi) Is it possible for the ICO to give additional guidance in its communications for (i)-(v) of the above please; e.g. Responding to a cybersecurity incident (ico.org.uk) It may be helpful to advise organisations to retain a clear log of actions, information

received, including expert advice relied upon, and decisions taken.

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?

BIBA Response:

107. This approach is not intended to be mechanistic. The overall assessment of the appropriate fine amount involves evaluation and judgement, taking into account all the relevant circumstances of the individual case. The guidance sets out details about each of the steps below.

(i) How does the ICO use case precedent to govern the outcome of similar cases? Is this available as public information? If the ICO does not use precedent, how does it judge different outcomes for similar cases?

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?

BIBA Response:

Would the ICO include information how to appeal a judgement/fine in order to support transparency.