Response to ICO consultation on the draft Statutory Guidance on Regulatory Actions

Submitted by Prof. Derek McAuley, Dr. Ansgar Koene and Dr. Jiahong Chen of Horizon Digital Economy Research Institute, University of Nottingham

11 November 2020

About this Guidance, Aims, Legislative basis and Regulatory Activity

Q1: Are these sections clear and easy to understand??

◉ Yes
○ No
○ Unsure/don't know

Q2: If no or unsure/don't know, why not? (use approximately 250 words)

Q3: Is there anything missing?

◉ Yes
○ No
○ Unsure/don't know

Q4: If yes or unsure/don't know, what other areas would you like to be covered in it? (use approximately 250 words)

1. The relationship between the Guidance and the Regulatory Action Policy should be made clearer not just in terms of the scope but also the nature of these two documents. Specifically, it should be highlighted upfront what precisely fall outside the remit of this Guidance but within that of the Policy (e.g. ePrivacy and Freedom of Information matters). It would also be helpful if the Guidance explicitly states what the 'statutory' status means, i.e. mandated by the DPA 2018 and subject to parliamentary approval.

2. The Guidance should also explain why the three matters governed by Sections 160, 133 and 158 are covered in one single guidance, especially considering the fact that the guidance required by Section 160 is subject to a more specific parliamentary approval procedure.

Information Notices

Q5: Is it clear and easy to understand?

◉ Yes
○ No
○ Unsure/don't know

Q6: If no or unsure/don't know, why not? (use approximately 250 words)

Q7: Is there anything missing?

◉ Yes
○ No
○ Unsure/don't know

Q8: If yes or unsure/don't know, what other areas would you like to be covered in it? (use approximately 250 words)

This section specifies that if an organisation fails to respond to an information notice on time, the ICO may apply for a court order or issue a penalty notice. While these two pathways are clearly provided for by the DPA 2018, there is nothing in the legislation preventing the ICO from serving an assessment notice as a further action in case of non-compliance with an information notice. This would be a potentially an alternative mechanism to allow the ICO to collect the information needed on site.

Assessment Notices

Q9: Is it clear and easy to understand?

◉ Yes
○ No
○ Unsure/don't know

Q10: If no or unsure/don't know, why not? (use approximately 250 words)

Q11: Is there anything missing?

◉ Yes
○ No
○ Unsure/don't know

Q12: If yes or unsure/don't know, what other areas would you like to be covered in it? (use approximately 250 words)

This section should also set out the factors to take into account when deciding what actions the ICO may take where an organisation fails to respond to an assessment notice.

Enforcement Notices

Q13: Is it clear and easy to understand?

◉ Yes
○ No
○ Unsure/don't know

Q14: If no or unsure/don't know, why not? (use approximately 250 words)

Q15: Is there anything missing?

○ Yes
◉ No
○ Unsure/don't know

Q16: If yes or unsure/don't know, what other areas would you like to be covered in it? (use approximately 250 words)

Penalty Notices

Q17: Is it clear and easy to understand?

◉ Yes
○ No
○ Unsure/don't know

Q18: If no or unsure/don't know, why not? (use approximately 250 words)

Q19: Is there anything missing?

◉ Yes
○ No
○ Unsure/don't know

Q20: If yes or unsure/don't know, what other areas would you like to be covered in it? (use approximately 250 words)

1. The assessment of the appropriateness of a penalty notice should also consider the benefits, including profits, gained by the organisation or individual concerned out of the breach. For certain organisations or even sectors, for example, the practices violating data protection law are central to their business model or day-to-day operation. In those cases, a fine would be especially necessary and effective (See Section 155(3)(k) & (l) DPA 2018).

2. This section should also specify the types of violations where the standard maximum amount and the higher maximum amount would respectively apply (See Article 83 GDPR and Section 157(2)-(4) DPA 2018).

Q21: Do you have any specific comments on the 9 step process to penalty setting? (use approximately 250 words)

1. The distinction between 'seriousness' and 'culpability' feels somewhat arbitrary, and certain factors currently categorised as a seriousness matter in fact have more to do with culpability, such as actions taken to mitigate damage, previous failures and compliance, and adherence to codes or certification mechanisms.

2. The table on page 23 is confusing in that it is meant to facilitate the calculation of the starting point of the fine, but the language in that table gives the reader an impression that it is calculating the maximum fine applicable. Please consider changing the terminology to, for example, 'standard penalty breaches' and 'higher penalty breaches'.

Fixed Penalties

Q22: Is it clear and easy to understand?

○ Yes
◉ No
○ Unsure/don't know

Q23: If no or unsure/don't know, why not? (use approximately 250 words)

It is not clear how the £400, £600 and £4,000 amounts have been determined. Section 158(3) DPA 2018 sets out the maximum amount of penalty to be '150% of the highest charge payable', whereas Regulation 3(1) of the Data Protection (Charges and Information) Regulations 2018 provides that the charge payable is £40 (micro organisations), £60 (small and medium organisations) and £2,900 (large organisations).

Q24: Is there anything missing?

◉ Yes
○ No
○ Unsure/don't know

Q25: If yes or unsure/don't know, what other areas would you like to be covered in it? (use approximately 250 words)

Please see answer to Q23 above.

Privileged Communications

Q26: Is it clear and easy to understand?

○ Yes
◉ No
○ Unsure/don't know

Q27: If no or unsure/don't know, why not? (use approximately 250 words)

This section simply repeats Section 133 DPA 2018 and has not provided any details on the ways the ICO will, for example, assess whether the communications concerned are privileged or what additional procedural measures will be put in place to ensure the ICO's obtaining of privileged communications (those not concerning data protection legislation) will respect the professional secrecy of the legal adviser.

Q28: Is there anything missing?

◉ Yes
○ No
○ Unsure/don't know

Q29: If yes or unsure/don't know, what other areas would you like to be covered in it? (use approximately 250 words)

Please see answer to Q27 above.

Effectiveness of Regulatory Action

Q30: Is it clear and easy to understand?

○ Yes
◉ No
○ Unsure/don't know

Q31: If no or unsure/don't know, why not? (use approximately 250 words)

This very brief section does not add any value to the Guidance and can be removed.

Q32: Is there anything missing?

○ Yes
◉ No
○ Unsure/don't know

Q33: If yes or unsure/don't know, what other areas would you like to be covered in it? (use approximately 250 words)

Evaluation and Next steps

Q34: Is it clear and easy to understand?

○ Yes
◉ No
○ Unsure/don't know

Q35: If no or unsure/don't know, why not? (use approximately 250 words)

This very brief section does not add any value to the Guidance and can be removed.

Q36: Is there anything missing?

○ Yes
◉ No
○ Unsure/don't know

Q37: If yes or unsure/don't know, what other areas would you like to be covered in it? (use approximately 250 words)

Miscellaneous

Q38: On a scale of 1-5 how useful is the draft guidance?

○ 1 - Not at all useful
○ 2 - Slightly useful
◉ 3 - Moderately useful
○ 4 - Very useful
○ 5 - Extremely useful

Q39: Why have you given this score? (use approximately 250 words)

Q40: To what extent do you agree that the draft guidance is clear and easy to understand?

○ Strongly disagree
○ Disagree
◉ Neither agree nor disagree
○ Agree
○ Strongly agree

Q41: Please provide any further comments or suggestions you may have about the draft guidance. (use approximately 250 words)