medConfidential comments on ICO Draft Data Protection Fining Guidance

1. Under this draft, a startup that breaches the law can argue they should not be fined because it would not be "dissuasive" of another startup from making the same breach (paragraphs 102-105). This response covers Circumstances and Hardship questions.

2. The guidance extends the difference in fining policy between the public and private sectors. We see nothing in this guidance which would make this discrepancy resilient to legal challenges, meaning that, over time, in the same way the ICO rarely imposes public sector fines, then the ICO will rarely impose any private sector fines either.

3. Therefore the guidance fails on its own terms as it fails to offer any incentives for compliance, let alone from those entities most likely to make the most egregious breaches. Indeed, it satisfies the Government goal of "co-designed with industry, for industry"[1] while the ICO places data subjects at unnecessary risk by giving up the only effective punishment the ICO has available.

4. We have covered elsewhere[2] that breaking the (Data Protection) law is a rational act for startups because a sign of great success is the company surviving long enough for regulators to investigate, determine, and issue any fine. As a result, in the context of the draft guidance, there can be no "specific" deterrence, there can be no "general" deterrence, as breaking the law continues to be the path of least resistance for other organisations who have few resources.

5. If you're a new tech startup, this guidance offers no impediment to stealing data and pleading poverty to the regulators. If you're a successful tech startup, it allows you to argue that a fine would not be dissuasive of competitor startups, and the fine would be disproportionately small to the size of the company by the time the fine was levied. Large firms would argue that they are being *disproportionately* penalised when a smaller company would not be fined.

6. As a thought experiment, the ICO may wish to examine how it would fine OpenAI for a personal data breach in chatGPT3 (a scenario where "Books3" had personal data[3]) – a company which at the time had no revenues, and a multi-billion valuation. The valuation of the company is not considered in current text, and the guidance should be explicit that it can be taken into account where applicable.

7. The guidance implies that a fine is unlikely where it would have zero dissuasive effect. Indeed, if the guidance is used to punish anyone, it will disproportionately punish the accountable and the honest and encourage them to be neither of those things, as the NHS saw with Babylon's 'innovations around truth' of their AIs.[4]

8. We have been unable to find a reason to describe this guidance as fit for purpose.

medConfidential

November 2023

---

[1] As described by HMG in bullet point 2, page 27: https://assets.publishing.service.gov.uk/media/654a21952f045e001214dcd7/The_King_s_Speech_background_briefing_notes.pdf#page=28

[2] https://www.disruptiveproactivity.com/2023/10/the-ai-summit/

[3] https://www.theguardian.com/books/2023/aug/22/zadie-smith-stephen-king-and-rachel-cusks-

[4] https://www.wired.co.uk/article/babylon-health-warning-ai-unicorns