Regulatory Action Policy; Statutory guidance on our regulatory action; and Statutory guidance on our PECR powers

About the policies

The first three questions are specific to each of the documents, for the remaining questions (questions 4 to 9) please identify the name of the document you are commenting on in your response.

1. Do you agree with our approach to how we exercise our regulatory responsibilities in the RAP? Please explain your answer.

Open Rights Group partially disagrees with the approach the ICO envisions in their Regulatory Action Policy: while we appreciate improvement and changes going in the right direction, we are still concerned that the ICO didn't take full stock of their failures to enforce the law in the past. As a result, the envisioned approach could still be gamed by bad-faith actors.

In turn, we explain what the changes that we believe are going in the right direction (1.1. What we liked), we then analyse problems that persist in this approach (1.2 Our concerns). Finally, we provide some examples to substantiate our position (1.3. Lessons from the past).

1.1.What we liked

We are glad to see that the ICO widened the scope and depth of their review of the Regulatory Action Policy. We also praise the stronger focus the new RAP places on dissuading bad-faith actors throughout the ICO regulatory processes. In particular, we support the decision to spell out "aggravating factors" to guide the ICO enforcement action holistically — as opposed to the existing RAP, that identifies aggravating factors for the specific purpose of "select[ing] the appropriate regulatory activity" —, as well as the inclusion of these particular aggravating factors:

- the attitude and conduct of the person or organisation concerned suggests an intentional, wilful or negligent approach to compliance or an unlawful business or operating model;
- the person or organisation did not follow relevant advice, warnings, consultation feedback, conditions or guidance from us or the data protection officer (for data protection cases);

- the person or organisation's prior regulatory history, including the pattern, number and type of complaints about the issue and whether the issue raises new or repeated concerns that technological security measures are not protecting the personal data.

As we stressed in our previous response to the draft Statutory Guidance consultation, we observed numerous instances where bad-faith actors exploited the ICO approach to regulation and relied on "industry engagement" processes to delay compliance and keep operating with impunity. Thus, we support and emphasise the need to consider conduct, regulatory history, and compliance with the inputs received during engagement processes to dissuade rogue actors from gaming the ICO engagement processes to their own advantage.

1.2. Our concerns

We emphasise that the ICO approach to regulation leans significantly toward using persuasion, education and other soft regulatory tools. In particular, by reading the section "How we help you comply with the legislation we monitor and enforce" together with other ICO regulatory documents, we understand the overall approach of the ICO as divided into several steps:

- Engagement with the public and the industry for general awareness raising about legal duties and obligations;
- Engagement with regulated entities during consultations on ICO regulatory guidances, and further engagement to promote awareness of finalised ICO Regulatory guidances and opinions;
- Engagement with industry in breach of data protection obligations with Investigative Reports, to raise awareness about regulatory shortcomings and give industry players the opportunity to address these concerns;
- Use of Statutory Powers to enforce the laws.

We also understand these steps to be conceived as sequential. Although anecdotal, this approach has been described by the ICO Executive Director of Regulatory Futures at "The Parliament and Internet Conference 2022", whose keynote equated enforcement actions as an indication of failure of the ICO in carrying out their function.

While we do agree that engagement and education play key roles in promoting data rights and compliance with the laws, applying such a step-by-step approach indiscriminately and to the letter would give leeways to abuse for bad-faith actors and organisations that want to operate in breach of data protection laws. In turn, this approach does not only risk condoning violations of individuals' rights and freedoms, but also fails to meet the duties of the ICO under the

Deregulatory Act 2015. Indeed, we draw attention on the following extracts of Statutory Guidance on the "Growth Duty":[1]

> *"1.4 Non-compliant activity or behaviour undermines protections to the detriment of consumers, employees and the environment and needs to be appropriately dealt with by regulators. It also harms the interests of legitimate businesses that are working to comply with regulatory requirements, disrupting competition and acting as a disincentive to invest in compliance.*
>
> *1.5 The growth duty does not legitimise non-compliance and its purpose is not to achieve or pursue economic growth at the expense of necessary protections. [...]"*

Thus, the ICO should not see "enforcement" as a failure, or in contrast with their aim of being "business-friendly". As clearly reflected by the growth duty, being "business-friendly" requires swift and effective enforcement against non-compliant businesses. Doing otherwise would expose law-abiding businesses to the unfair competition of free riders and bad-faith actors.

1.3. Lessons from the past

We substantiate our concerns expressed in §1.2 by providing two examples where the ICO failed to adapt their approach to the regulated subjects' circumstances and attitudes. In turn, this left data rights violations unaddressed and marked failures against their duty to uphold data rights and promote compliance among the industry.

The UK Government response to coronavirus:

In the aftermath of the Coronavirus outbreak, the UK Government initiated the development of a digital contact tracing application, raising numerous concerns in the field of data protection.[2] The ICO response was to engage with the Government and release an opinion to promote Government compliance with data protection in the development of contact tracing applications.[3]

---

1 Available from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/603743/growth-duty-statutory-guidance.pdf

2 See ORG Response to the "Science of Covid" consultation of the Lords' Science and Technology Committee. Available from: https://www.openrightsgroup.org/publications/response-to-the-science-of-covid-consultation-of-the-lords-science-and-technology-committee/

3 See ICO COVID-19 Contact tracing: data protection expectations on app development. Available from: https://ico.org.uk/media/for-organisations/documents/2617676/ico-contact-tracing-recommendations.pdf

Later on, Open Rights Group revealed that the UK Test and Trace programme was being carried out illegally, lacking a Data Protection Impact Assessment.[4] Following the admission by the lawyers of the Department of Health and Social Care about the illegality of Test and Trace, the UK Government openly stated their intention not to comply with the law, and in particular, the Secretary of State for Health held that "[the Government] won't be held back by bureaucracy".[5] Regardless of these circumstances, the ICO adopted once again a "critical friend" attitude.[6] This failure to identify and mitigate risks associated with the processing of Test and Trace data produced tangible harms to individuals, such as

- women being harassed via contact info collected for contact tracing purposes;[7]
- leakage of contact tracing personal data to social media platforms — such as in the case of contact tracing volunteers using Facebook groups to share this data among themselves;[8]
- a number of data breaches in England,[9] in Wales,[10] and after the vaccine rollout.[11]

In summary, the UK Government consistently displayed bad faith toward complying with legal obligations.[12] Their attitude did not change after the ICO

4 See BBC, Coronavirus: England's test and trace programme 'breaks GDPR data law'. Available from: https://www.bbc.com/news/technology-53466471

5 Recorded statement available at this link: https://twitter.com/OpenRightsGroup/status/1285260608875700225?s=20

6 See The Independent, Coronavirus: England's test and trace programme 'breaches data laws', privacy campaigners say. Available from: https://www.independent.co.uk/news/health/coronavirus-test-trace-england-privacy-security-a9627691.html

7 See The Telegraph, Test and trace is being used to harass women – already. Available from: https://www.telegraph.co.uk/women/life/test-trace-used-harass-women-already/

8 See The Times, Coronavirus contact tracers sharing patients' data on WhatsApp and Facebook. Available from: https://www.thetimes.co.uk/edition/news/coronavirus-contact-tracers-sharing-patients-data-on-whatsapp-and-facebook-rg3zqn5l6

9 https://www.bbc.com/news/uk-52732818

10 https://www.digitalhealth.net/2020/09/public-health-wales-data-breach-covid-19/

11 https://bigbrotherwatch.org.uk/2021/05/the-guardian-publics-vaccination-status-leaked-by-nhs-booking-site/

12 ORG Test and Trace briefing for JCHR. Available from: https://www.openrightsgroup.org/publications/test-and-trace-briefing-for-jchr/

"engaged" with them, as they reacted by publicly boasting themselves for disregarding the law. The ICO, however, did not react to such developments and allowed the Government to keep operating illegally. As a result, individuals suffered data rights violations and tangible harms.

The Adtech industry and Real Time Bidding:

In 2016, the EU formally approved the GDPR, providing a two-year grace period for businesses to bring their activities in line with the law. In 2017, the Interactive Advertising Bureau wrote to the European Commission to lament that the data protection regime being discussed in the GDPR would have made their business model illegal.[13]

The IAB did not implement any significant change to their advertising model, as revealed by the complaint submitted by Dr. Johnny Ryan, Jim Killock from Open Rights Group and Micheal Veale from University College London in 2018. The ICO issued an "adtech update report" in 2019, validating these arguments and announcing that they would have engaged with the industry to start the reform of the adtech sector.[14] This process led to no tangible results, and the ICO released an opinion in 2021 on "Data protection and privacy expectations for online advertising proposals", where they reiterated the same concerns.

In the meanwhile, the same adtech complaint was lodged in 21 EU jurisdictions and investigated by the Belgian Data Protection Authority. Despite the significant procedural hurdles stemming from the EU cross-border consistency mechanism, in February 2022 the Belgian APD ordered the IAB to bring their operations into compliance.[15] The decision is now pending judicial appeal.

In summary, the IAB was aware that their RTB systems were in breach of data protection laws since 2017. Nevertheless, in over 6 years the IAB consistently refused to take any meaningful action to comply with legal requirements. Failure from the ICO to adapt their approach even before obvious and reiterate displays of bad faith resulted in:

- A 4 years-long failure to uphold data rights in the field of online advertising;

---

13 See New evidence to regulators: IAB documents reveal that it knew that real-time bidding would be "incompatible with consent under GDPR". Available from: https://brave.com/update-on-gdpr-complaint-rtb-ad-auctions/#evidence

14 ICO Blog: Adtech - the reform of real time bidding has started and will continue. Available from: https://ico.org.uk/about-the-ico/news-and-events/blog-adtech-the-reform-of-real-time-bidding-has-started/

15 Belgian APD, The BE DPA to restore order to the online advertising industry: IAB Europe held responsible for a mechanism that infringes the GDPR. Available from: https://www.dataprotectionauthority.be/citizen/iab-europe-held-responsible-for-a-mechanism-that-infringes-the-gdpr

- Delays in regulatory enforcement in comparison to EU Data Protection Authorities, even where the latter face significant hurdles from the need of cross-border coordination;
- Legitimate online advertising businesses facing unfair competition from adtech intermediaries that participate to real-time-bidding.

2. Do you agree with our approach to how we exercise our statutory powers in the statutory guidance on our regulatory action (pursuant to our obligations under s160 DPA 2018)? Please explain your answer.

We are worried that some of the improvements to the Regulatory Action Policy do not seem to be appropriately reflected in the Statutory Guidance. We also believe that the ICO should draw inspiration from the competing and more successful approach the Belgian APD have shown in their adtech investigation handling.

While we praise the clear references in the RAP to the conduct, regulatory history, and compliance of regulated entities with the inputs received during engagement processes, the wording of the criteria to issue Information, Assessment, Enforcement and Penalty notices appear to be less robust.

Furthermore, we wish to draw attention to the differences in approach between the ICO and the Belgian APD, following their investigation reports on adtech. On the one hand, the ICO gave an informal six-month notice to work on the points raised in the report, but in §1.3, this did not materialise in any meaningful result. On the other hand, the Belgian APD reacted to the investigation findings by escalating the issue to the litigation chamber, which eventually adopted an enforcement decision that also included a six-months period to comply.

We ought to emphasise that both authorities produced an investigation report and then sought to give regulated entities a grace period to address the issues uncovered in these reports. However, the Belgian APD notably decided to support their attempt to promote compliance in the adtech industry with an enforcement notice, which would deter regulated entities' attempts to game engagement processes. We believe this approach presents significant advantages when industry players are not showing a genuine attitude to collaboration.

3. Do you agree with our approach to how we exercise our statutory powers in the statutory guidance on our PECR powers (pursuant to our obligations under s55C DPA 1998)? Please explain your answer.

/

4. Is there anything you would do differently in terms of our approach? Please explain your answer.

Our recommendations are to amend the Regulatory Acton Policy and draft Statutory Guidances in the following manners:

1. To amend references to the Deregulation Act 2015, in line with the Draft Statutory Guidance issued under Section 110(6) of the Deregulatory Act 2015. In particular, the Regulatory Action Policy should fully reflect its prescriptions that "Non-compliant activity or behaviour undermines protections" and "harms the interests of legitimate businesses that are working to comply with regulatory requirements" and thus "the growth duty does not legitimise non-compliance and its purpose is not to achieve or pursue economic growth at the expense of necessary protections".

2. To expressly acknowledge that businesses may not genuinely engage with the ICO to bring their activities into compliance, and that the ICO should adopt a more assertive approach toward Statutory Enforcement when this happens, in line with their duty to uphold the law and promote the growth of law-abiding businesses. Ideally, this would be supported by a set of criteria to identify organisations that are not engaging in good-faith with the ICO;

3. To streamline the draft Statutory Guidances to the changes recommended in points 1 and 2 above, and in particular by referencing these changes and the criteria we highlighted in §1.2 of our response to the sections "When would we issue an information, enforcement, penalty notices";

4. To amend the draft Statutory Guidance in a way that allows the use of enforcement notices as a support for engagement with the industry, as argued in §2. For instance, where an industry-wide investigation were to reveal systemic breaches of data protection laws, issuing an enforcement notice to bring activities into compliance with the law within a given timeframe could be leveraged as a deterrent against organisations that may want to game the ICO approach to avoid having regard of the findings of the findings of that investigation.

5. How much do you agree with the following statements:

"The purpose of the RAP is clear"

- [ ] Strongly agree
- [ ] Agree
- [ ] Undecided
- [ ] Disagree
- [ ] Strongly disagree

"The purpose of the statutory guidance on our regulatory action is clear"

- [ ] Strongly agree
- [ ] Agree
- [ ] Undecided
- [ ] Disagree
- [ ] Strongly disagree

"The purpose of the statutory guidance on our PECR powers is clear"

- [ ] Strongly agree
- [ ] Agree
- [ ] Undecided
- [ ] Disagree
- [ ] Strongly disagree

6. How much do you agree with the following statements:

"The RAP is helpful"

- [ ] Strongly agree
- [ ] Agree
- [ ] Undecided
- [ ] Disagree
- [ ] Strongly disagree

"The statutory guidance on our regulatory action is helpful"

- [ ] Strongly agree
- [ ] Agree
- [ ] Undecided
- [ ] Disagree
- [ ] Strongly disagree

"The statutory guidance on our PECR powers is helpful"

- [ ] Strongly agree
- [ ] Agree
- [ ] Undecided
- [ ] Disagree
- [ ] Strongly disagree

7. Do you have any suggestions on how we could make the documents clearer or more helpful?

/

8. Are there any issues in the documents that you would like us to cover more thoroughly?

/

About you:

9. What is your name?

Mariano delli Santi

10. What is your email address?

mariano@openrightsgroup.org

11. Who are you responding as?

- ☐ An individual
- ☒ On behalf of an organisation

12. What is the name of your organisation?

Open Rights Group

13. Which sector do you represent?

- ☐ Private
- ☐ Public
- ☒ Third

14. What industry does your organisation fall into?

- ☐ Education
- ☐ Social services
- ☐ Police/Emergency services
- ☐ Environment
- ☐ Leisure services
- ☐ Healthcare
- ☐ Armed forces
- ☐ Civil service
- ☐ Politics/Local government
- ☐ Utilities
- ☐ Rail/Road/Airline
- ☐ Recruitment
- ☐ Construction/Property
- ☐ Retail/Food

- ☐ Banking/Finance
- ☐ Law/Legal
- ☒ Charity
- ☐ Other

Privacy

15. We may decide to publish your name or the name of the organisation you are responding on behalf of or both, to indicate that you have responded to our consultation. Please indicate whether you consent to us publishing your name or the name of the organisation you are responding on behalf of or both for this purpose.

- ☒ I consent to you publishing my name and the name of my organisation to indicate I responded to this consultation.
- ☐ I consent to you publishing my name to indicate I responded to this consultation.
- ☐ I consent to you publishing the name of my organisation to indicate I responded to this consultation.
- ☐ I do not consent to you publishing my name or organisation to indicate I responded to this consultation.

Before you submit:

16. How did you hear about the consultation?

I follow the work of the ICO on a regular basis.

17. How satisfied are you with the consultation?
(1 = very satisfied, 2 = satisfied, 3 = neither satisfied or unsatisfied, 4 = unsatisfied, 5 = very unsatisfied)

1	2	3	4	5
☐	☐	☐	☒	☐

18. Are there any ways you would change the survey (ie type of questions, style of question, format, methods to respond)?

I didn’t find the tick-box questionnaire to be particularly useful to comment the document being consulted.