RESPONSE TO THE ICO CALL FOR VIEWS ON ENFORCEMENT PROCEDURAL GUIDANCE

Submission – January 2025

Author: Mariano delli Santi mariano@openrightsgroup.org

In this response

2.4. Do you have any comments on the alternative means we may use to resolve a matter other than opening an investigation?

1 While using means other than an investigation to resolve a matter may be appropriate at times, the guidance outlines an approach that risks becoming smokes and mirrors to avoid using corrective powers as intended under UK data protection law.

2 It is worth pointing out that the ICO is responsible, under Article 51 of the UK GDPR, for the "monitoring the application of this Regulation, in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data". As stated by the consultation document, the ICO also has a duty to act fairly and reasonably, consistent with the UK public sector duty. Thus, it is only logical that the appropriateness of any regulatory action the ICO takes must be assessed against its effectiveness in ensuring the application of UK data protection law and the protection of individuals' rights. Indeed, the ICO Regulatory Action Policy, which the guidance under consultation seeks to replace, states that regulatory action is taken "with a view to *guaranteeing* that individual's information rights are properly protected" and that "any regulatory action is targeted, propionate and *effective*" [emphasis added].

3 Further, in *Delo vs. Information Commissioner*, the Administrative Court recognised that the ICO has discretion to exercise its functions, but validated the use of such discretion on the basis that the ICO reached a "rational decision". The judgment also identified some factors against which such rationality to not pursue an investigation has to be assessed against, namely:

3.1 The likely outcome of further investigation;
3.2 The likely merits [of the case];
3.3 Any alternative methods of enforcement that are available to the data subject.

4 Against this background, the guidance under consultation provides overly vague statements that leave the use of the Commissioner's discretion unchecked and unpredictable. This leaves little to no assurance that the ICO is going to decide whether to open an investigation on rational grounds, ie. with a view on adopting a response that protects individual rights and is effective. This risk appears particularly acute in **the following remedies, listed in paragraph 33 of the guidance**:

5 **Accepting assurance to remedy compliance concerns:** The guidance states that the ICO would be willing to accept assurances about steps the offender "has taken or will shortly take", such as "committing to implement measures to improve compliance" and "providing redress for any damage or distress people may have suffered". This language suggests that the ICO may decide not to take action where harm or distress has occurred or is still ongoing.

6 As stated before, the ICO has, as a public body, an overarching duty to act fairly and reasonably. However, accepting assurances where non-compliant and thus harmful conduct is still ongoing would constitute a rather unfair and unreasonable conduct. The same can be said in the event where an infringing behaviour has already stopped, but a decision not to exercise corrective powers would fail to deter further non-compliance. Either way, the guidance fails to articulate a criteria or a threshold to determine whether accepting an assurance or an undertaking would be compatible with the objectives of dissuading non-compliant behaviour and ensuring compliance with UK data protection law more generally.

7 **Referring the issue to another public body that may be better placed to deal with it:** Such an alternative to opening an investigation is nonsensical. The ICO is the only authority in the UK with remit to oversee compliance with UK data protection law, with a few exceptions which include intelligence services processing and processing carried out by judicial bodies. Within this scope, there is no other public authority that has the power to ascertain that an infringement has happened and ensure compliance with relevant legal standards.

8 Breaches of data protection legislation may also constitute relevant conduct under other regulatory regimes. For instance, forcing individuals to consent to commercial uses of data would be both a breach of data protection law and an unfair commercial practice. Even if this was the case, the interplay between different regulatory regime does not authorise the ICO to step down from its regulatory function. Even if another authority was in the position to intervene —in this example, to address an unfair commercial practice—their would still be the need, and the ICO would have a duty to, act upon a violation of UK data protection law, and ensure that infringement behaviour is addressed accordingly.

9 Once again, this statement also seems to diverge significantly from the ICO Regulatory Action Policy (RAP), which recognises "the interconnected landscape of the technological aspect in which we operate" and states that "Where we undertake joint regulatory or investigative work, we coordinate our activity to ensure a proportionate burden on those being regulated". Thus, while the RAP foresees joint work and coordination with other regulatory

authorities, it never suggest the ICO would forfeit its regulatory functions as a consequence of it.

Recommendations

10 The guidance should include clear language that clarifies the ICO will determine whether to open an investigation or rely on alternative means to resolve a matter with a view to guaranteeing the protection of individuals' rights and ensuring compliance with UK data protection law.

11 The guidance should also clarify how the Commissioner will assess if and how an alternative mean to resolving an investigation would be effective for ensuring the monitoring and application of UK data protection law and the protection of individuals' rights.

12 The guidance should be amended to clarify that assurances will never be accepted as a reason not to open a formal investigation unless there is evidence that shows the infringing conduct has already stopped, and that the likelihood of repeated offence is remote. Ideally, the guidance would also substantiate the evidentiary test needed.

13 The guidance should scrap the step "Referring the issue to another public body that may be better placed to deal with it" and replace it with a statement which aligns with the "Working with others to take effective action" statement enshrined in the ICO Regulatory Action Policy. This statement should clarify that the ICO will not forfeit its statutory duties when a data protection matter under the remit of the ICO also falls within the remit of another regulatory authority.

2.5 Do you have any other comments on the section "How we decide whether to open an investigation"?

14 **Paragraph 35 of the guidance** outlines a number of cases where the ICO "may decide not to open an investigation or take any other steps". Some of these statements suggest that the ICO may disregard its duty to ensure the application of UK data protection law and the protection of individuals' rights, while others fail to establish criteria or a framework against which the ICO performance can be predicted, assessed or held to account.

15 In general, the section outlines a number of hypothetical scenarios where the ICO may decide not to take any action, based on what may be considered

appropriate by the ICO themselves. By failing to establish clear criteria and threshold as to when the ICO would take action, or would rely on one option rather than another, the whole section fails to establish criteria against which the ICO conduct could be assessed and held to account, thus establishing arbitrary and unreasonably broad discretion for the ICO in the performance of its functions. In detail:

16 **The statement within the second criteria**, according to which "the scale of any harm […] does not merit any further action based on the factor we use to prioritise work", is inappropriate and, likely, unlawful. The ICO has a duty to ensure the application of UK data protection law and the protection of individuals' rights; thus, it would be unfair and unreasonable not to open an investigation based on the subjective point of view of the ICO. Pursuing "strategic objectives", or whatever lingers in the minds and private interests of the ICO and its leadership, cannot and should not interfere with the pursuit of statutory functions enshrined in legislation.

17 It is also worth mentioning that the Data (Use and Access) Act introduces changes that require the ICO to "prepare a strategy for carrying out the Commissioner's functions under the data protection legislation in accordance with the Commissioner's duties under" sections 120A and 120B of the UK Data Protection Act. The language "in accordance with its duties" clarifies that the ICO strategy cannot override the interests enshrined in legislation. Thus, the ICO organisational priorities are not a legitimate ground for overriding the duty to enforce UK data protection law and protect individuals' rights.

18 **The fourth criteria**, according to which "we consider that we are not best placed to act" is nonsensical. As mentioned before (see *supra*, Paragraphs 7-9), legislation establishes the remit where the ICO has a duty to oversee regulatory compliance. If the ICO considers such remit to be inappropriate, it should report to Parliament and make the case for what changes under UK data protection law are warranted and why.

19 **The statement within the second criteria**, according to which "the scale of any harm appears too low to merit further action" implies that non-compliant conduct would not be investigated or dealt with even where harm was occurring and had not stopped. This cannot be right, and would be manifestly unlawful if this were the meaning intended by this guidance.

20 **The third criteria**, according to which "we are satisfied that the controller or processor has already taken appropriate steps […] and we do not consider any further action is appropriate" fails to articulate how the ICO means to comply with its duty to dissuade non-compliance with data protection law. Even if a

non-compliant conduct has ceased, opening an investigation and using corrective powers may be needed, in particular where:

20.1 The non-compliant conduct may be a symptom of further or deeper failings to comply with UK data protection law, and thus may warrant an investigation;

20.2 Issuing an enforcement notice may still be needed to hold a previously non-compliant controller or processor to account if they later were to walk back or repeat their offensive conduct.

20.3 Even where there was no indication or reason to believe the controller or processor responsible for the infringing behaviour would repeat their offence, issuing a reprimand or a penalty notice would constitute an appropriate response to dissuade non-compliance in general.

Recommendations:

21 The guidance should scrap the statement according to which the ICO would not take further action based on its organisational priorities. If the ICO aims to give clarity as to how they would factor the growth duty under the Deregulation Act 2015, or duties under Section 120B of the UK DPA, the guidance should state this clearly and articulate

21.1 How the Commissioner would factor these interests in a decision not to take any further action;

21.2 How this decision would be measured against the overarching duty to ensure compliance with UK data protection law and protect individuals' rights.

22 The guidance should scrap the statement that the ICO would not take action if "we consider that we are not best placed to act" and replace it with a statement which aligns with the "Working with others to take effective action" statement enshrined in the ICO Regulatory Action Policy. This statement should clarify that the ICO will not forfeit its statutory duties when a matter under the remit of the ICO also falls within the remit of another regulatory authority.

23 The guidance should scrap the statement that the ICO would not take action if "the scale of any harm appears too low to merit further action". If the ICO believes that there is an alternative and more effective remedy that makes its intervention unnecessary, the ICO should commit to state what those remedies are and provide a clear assessment of how the comply with the duty to ensure the effective application of UK data protection law

3.1. Do you have any comments on the process to be followed when opening an investigation?

24 In general, the guidance never articulates how and according to which criteria the ICO would determine that not pursuing an investigation where evidence suggest non-compliance would be fair and reasonable. The same holds true for what circumstances would or would not justify the ICO own priorities to override the public's information rights or the statutory function assigned to the ICO by UK data protection law. As such, the guidance fails to establish any meaningful criteria or threshold against which the ICO decision to open or not to open an investigation can be measured and held to account. In detail:

25 **The guidance states at paragraph 39** that "If we open an investigation, it means that we are satisfied the available evidence merits doing so and the issue is a priority". Such statement is deeply problematic:

25.1 **Firstly**, the guidance does not explain or articulate what are the criteria or the threshold that would make the ICO "satisfied" that an investigation is warranted. This omission runs contrary to *Delo vs. Information Commissioner*, where the Administrative Court found that the rationality and lawfulness of the ICO decision not to investigate a complaint were to be found in the absence of evidence that a wrongdoing had been committed, and the summarily manifest legality of the conduct the complainant had described. The judgment does not state the ICO would have discretion not to pursue an investigation if evidence of a wrongdoing or an infringement were present, nor it appears that such a conduct would be compatible with the overarching public sector duty to act reasonably and fairly.

25.2 **Secondly**, the guidance states that the ICO would open an investigation if "the issue is a priority". While the guidance does not state on which basis the ICO may or may not consider an issue to be a priority, previous sections suggest the ICO would refer to its own "strategic objectives" (see *supra*, paragraphs 7-9). As explained in that instance, it is unreasonable, unfair and without grounding in UK data protection law for the ICO to place its own motives before the performance of statutory functions.

26 **Finally, paragraph 47 of the guidance states that**, if the ICO had sufficient information "to reach a provisional decision that a controller has, or continues to, infringe" UK data protection law, the ICO "may give a notice of intent to give a penalty notice or a preliminary enforcement notice". The guidance uses "may" and the conditional mood without giving the actual conditions upon

which they *would do* what the guidance states. As such, the statement lacks meaning and leaves the ICO arbitrary and unaccountable discretion over when to issue a notice or not.

Recommendations:

27 The guidance should be amended to clarify when the ICO will open an investigation, instead of when the ICO may (or may not) do something. Ideally, such guidance would articulate how the ICO would assess if the evidentiary threshold has been met for suspecting that an infringement has occurred and an investigation is warranted.

28 The guidance should remove reference to the ICO strategic priorities as a ground to open an investigation. If the ICO wants to provide clarity as to how it would factor objectives enshrined in the Deregulation Act 2015, or Section 120B of the UK DPA, the guidance should provide a statement to clarify that, and assess the compatibility of these choices against the overarching duty to ensure compliance with UK data protection law.

3.3. Do you have any comments on our approach to engaging with controllers and processors during an investigation?

29 **Paragraph 61 of the guidance** states that the ICO, after considering representations from the controllers, "may decide not to take enforcement action at this state" if "the issue could be resolved through other means". This statement fails to articulate what the "other means" would be, and against which criteria they would be judged appropriate to resolve an issue identified during an investigation.

30 The same paragraph also states that the ICO may not take action if "the matter is no longer a priority", referring to section 2.4. Considerations made before (see *supra*, paragraphs 7-9) ought to be repeated with regard to this statement. The ICO own organisational needs cannot be relied upon to shy away from statutory duties.

Recommendations:

31 The guidance should clarify what conditions would need to be met for not taking action based on a representation given by a controller or processor, and

how this choice would adhere to the duty to ensure application of UK data protection law and the protection of individuals' rights.

32 The guidance should remove reference to the ICO strategic priorities as a ground not to open an investigation on the basis of a controller or processor's representations. If the ICO wants to provide clarity as to how they would factor objectives enshrined in the Deregulation Act 2015, or Section 120B of the UK DPA, the guidance should provide a statement to clarify that and assess the compatibility of these choices against the overarching duty to ensure compliance with UK data protection law.

4.1. Do you have any comments on our approach to the use of information notices and urgent information notices?

33 **Paragraph 72 of the guidance states** that "We may require a controller or processor to provide us with information or documents that we reasonably require to carry out functions under data protection law". The use of the modal verb "may" is deeply problematic, as it suggests there may be instances where the ICO would not require a controller or processor to provide information or documents which are necessary to carry out functions under data protection law. A policy so construed summarily appears to be irrational, as it is difficult to envision an occurrence where it would reasonable for the ICO not to require documents it needs to carry out its public functions.

34 **Paragraph 78 of the guidance** lays out a number of condition upon which the ICO may give a longer timescale to the recipient of an information notice in order to answer such request. While it may appear sensible on the surface, this statement overlooks that controllers have a duty to demonstrate compliance, pursuant to Article 5(2) and 24(1) of the UK GDPR. Thus, it would appear more appropriate for the ICO to leave it to the controller to prove that they may need more than 28 days to answer a request, and give a 28 days timescale by default unless such proof is given.

35 **Paragraph 91 of the guidance states** that failure to provide adequate and accurate information in response to an information notice "without a reasonable excuse may lead to us taking enforcement action and imposing a fine". Once again, the use of the modal verb "may" results in an overly vague statement that gives unchecked discretion over how the ICO would or would not act if they were provided false information. Ultimately, the guidance fails to explain why and in what circumstances would it be justifiable not to act against a recipient who provides false information "without a reasonable excuse".

36 It is also worth mentioning that the above marks a significant divergence from the ICO Regulatory Action Policy, according to which "If a recipient of an information notice does not fully respond within the applicable time period, whether urgent or not, the Commissioner will promptly apply for a court order requiring a response". The RAP also lists a number of criteria according to which the Commissioner would not apply for a court order, which are generally grounded on the information being required in the notice not being useful any longer. All considered, the RAP policy appears to describe a rational and logical policy which supports the pursuit of the ICO statutory functions. The case for overriding this policy with vague statements that are liable of contradicting the ICO duties under the law is unclear, and has certainly not be made.

Recommendations:

37 The guidance should retain relevant sections of the Regulatory Action Policy that explain when and according to which criteria the Commissioner will apply for a court order against a failure to comply with an information notice.

38 The guidance should focus on when the Commissioner will issue an information notice, and how this would be used to gather information useful for the investigation, instead of providing vague statements as to when the Commissioner may (or may not) do something.

39 Ideally, the guidance would clarify that the Commissioner will require an information notice to be answered within 28 days, and that it is up to the recipient to request an extension and articulate why it would be needed to answer to the request.

4.2. Do you have any comments on our approach to the use of assessment notices and urgent assessment notices?

40 **Paragraph 108 of the guidance** states that "If a recipient does not comply with a requirement in an assessment notice", the ICO may "apply for a court warrant" or "take enforcement action by imposing a fine". This statement is generally vague and, most notably, does not explain when and according to which criteria the ICO would decide that a recipient should not face a court order or a fine for failing to comply with an assessment notice. It is worth remembering that complying with an assessment notice is a legal obligation

under UK data protection law, and the ICO does not have power to exempt controllers from legal obligations established by UK law.

Recommendations:

41 The guidance should state that the Commissioner will apply for a court warrant against a failure to comply to an assessment notice, unless there is no further need to investigate the recipient. Ideally, the guidance would state criteria to determine when the decision not to issue an investigation would be compatible with the ICO overarching duty to ensure the application of UK data protection law and the protection of individuals' rights.

42 The guidance should clarify when the Commissioner would impose a fine to a recipient who fails to comply with an assessment notice. Ideally, the statement would articulate how the decision not to fine the offender would fare against the need to ensure the ICO regulatory action is dissuasive and effective.

4.3. Do you have any comments on our approach to requesting reports from approved persons as part of an assessment notice?

43 **Paragraph 149 of the guidance** states that "In determining the suitability of an approved person, we may take into account" a given list of factors. The use of the modal verb "may" is inappropriate, as it implies the ICO may not take into account such factors. Determining the suitability of an individual without having regard of, for instance, "the skills, expertise, experience and relevant qualifications" or if "there are any conflict of interest" is, however, clearly unreasonable and irrational.

Recommendations:

44 The guidance should drop the use of *may* and clarify, instead, how an approved person *should* look like, and what this is ultimately meant to *ensure*.

6.1. Do you have any comments on our approach to closing investigations on the basis of our priorities, resolving the issues through other means, or there being no grounds for action?

45 **Paragraph 208 of the guidance** states that the ICO "may decide: to close the investigation based on our priorities or because we have decided to resolve the issue through other means", which ""may among other things include providing advice or recommendations or accepting assurances". This is further substantiated by **paragraph 215**, which states that a relevant factor the ICO would take is "wether we could allocate our resources more appropriately to other work, particularly if we would need to put in significant further effort to continue the investigation".

46 This statement appears deeply problematic:

46.1 **Firstly**, the law provides the ICO with a degree of discretion in the monitoring and application of UK data protection law. However, the law and relevant case-law never authorises the ICO to give up its oversight role or exempt controllers from consequences for non-compliance on the ground that the ICO may find it difficult or onerous to perform its functions.

46.2 **Secondly**, the guidance does not measure the appropriateness of relying on "advice" or "recommendations" or "assurances" against obvious criteria, such as whether these methods would be suitable to uphold information rights and remedy the infringement being investigated.

Recommendations:

47 The guidance should scrap references to the ICO strategic priorities and the effort required to the ICO as a ground for closing an investigation.

48 The guidance should articulate the criteria the ICO would use to assess whether closing an investigation, or relying on alternative means, would comply with relevant statutory duties such as ensuring the application of, and compliance with, UK data protection law, protecting individuals' rights, and upholding information rights in the public interest.

7.1. Do you have any comments on our approach to giving warnings?

49 **Paragraph 227 of the guidance** states that, in the event where the ICO would serve a warning, and "if the controller or processor still commences the relevant processing operations in a way that we consider infringes data protection legislation, we may regard its failure to take into account the warning as an aggravating factor when we are considering what, if any, steps to take". This statement is unreasonable, since:

49.1 A recipient which defies a warning and still commences a processing operation which infringes UK data protection law would be acting with intent and bad-faith. Since the ICO has a duty to act fairly and reasonably, such an event must not only trigger enforcement action, but has to be regarded by the ICO as an aggravating factor.

49.2 Mindful of the above, the language "what, if any, steps to take" suggest that the ICO may not take action before a controller or processor who purposefully acts in bad-faith and breaches data protection legislation. While we appreciate the ICO has a degree of discretion in determining how to react to an infringement, such a behaviour would be manifestly irrational and incompatible with the ICO public sector duty.

Recommendations

50 Guidance over how the ICO uses warnings should be rewritten to ensure consistency with the aims of dissuading the recipient of a warning from going ahead and infringing UK data protection law. This should, at a bare minimum, articulate what (not *if*) regulatory intervention will the ICO take if a recipient disregards a warning and commits an infringement. Ideally, the guidance would also articulate how effectiveness and dissuasion would be assessed in this scenario.

8.1. Do you have any comments on our approach to giving reprimands?

51 **Paragraph 236 of the guidance states** that the ICO may give a reprimand "if we consider that: [...] in accordance with our approach to public sector enforcement, a penalty notice is not appropriate in the circumstances". This statement is problematic in that it implies that reprimands would be the only alternative to issuing a fine against a public sector body.

52 As reprimands lack the force of law, reasonableness dictates that their use should be limited to circumstances where the gravity of the infringement is low, the conduct has already ceased, and the likelihood of a repeated offence remote. In most circumstances, the reasonable alternative to a penalty notice should be an enforcement notice, which does not only legally bind the recipient to address the compliance matters identified, but can also be used in court to hold the recipient to account if they fail to do so.

53 **Further, paragraph 246 of the guidance states** that "Alongside the reprimand, we may also provide recommendations to assist the controller or processor in ensuring that its processing does not infringe data protection legislation and to maintain compliance. These recommendations do not form part of the reprimand and are not legally binding. Therefore, any decision by the controller or processor to follow our recommendations is voluntary". This statement is extraordinary on account that:

53.1 **Firstly**, it states that these recommendation would not be legally binding because they would not be part of a reprimand. This implies that if they were part of a reprimand they would be legally binding. As reprimands lack the force of law, this statement misrepresents what a reprimand is.

53.2 What the guidance does not state, however, is that these recommendations would not be published alongside the reprimand, since they would not be part of it. It follows that the public would not have knowledge of what recommendations have been issued to a given offender, and would thus not be able to appreciate if they are complying with them.

53.3 **Secondly**, the issuing of a reprimand alongside some "voluntary" recommendations is, in essence, an attempt to construe an enforcement remedy that is not provided by UK data protection law, which replicates an enforcement notice in all but its legally binding nature. The rationale for inventing an "enforcement notice" that cannot be enforced is manifestly flawed and, in any case, it would be up to Parliament and not the ICO to introduce new remedies in UK data protection law.

53.4 **Thirdly**, the rationale which underpins an enforcement notice is to address non-compliance: if a controller or processor are found to be infringing data protection legislation, an enforcement notice articulates what changes need to happen to address that infringement. Since they are legally binding, they ensure that the recipient will implement them and thus comply with UK data protection law, or they allow to hold to account them if they disregard these obligations.

53.5 The ICO is, however, proposing an approach where, facing an infringement of data protection law, they would issue a non-binding reprimand alongside some, equally non-binding recommendations. This leaves the recipient of these recommendations free to disregard them and continue with their non-compliant behaviour. This is summarily irrational and unreasonable. In any case, the guidance fails to articulate in what way would such an approach comply with the public sector duty the ICO is subject to.

Recommendations:

54 Guidance regarding the ICO approach to issuing reprimands should be scrapped and rewritten from scratch. The new guidance should be consistent with the nature of reprimands, which lack the force of law and, thus, cannot remedy an infringement which is ongoing, nor they are suitable for ordering compliance measures or preventing an infringement from happening again. At a bare minimum, the new guidance should:

54.1 Limit the use of reprimands to cases where the gravity of the infringement is low, the conduct has already ceased, and the likelihood of a repeated offence remote;

54.2 Articulate how the Commissioner would assess that a reprimand is sufficient to ensure the application of UK data protection law, and why an enforcement or penalty notices would not be needed.

55 Finally, the new guidance should drop any reference to the use of voluntary recommendations attached to a reprimand. If the Commissioner considers such remedy useful and necessary to perform their function, they should report to Parliament and make the case for their inclusion in UK data protection law.

9.1. Do you have any comments on the factors we consider when deciding to give an enforcement notice or an urgent enforcement notice?

56 **Paragraph 254 of the guidance** states that the ICO "can give an enforcement notice to a controller or processor", and then proceeds to list the compliance failures against which an enforcement notice could be issued. It then substantiate, in **paragraphs 258 and 259**, the factors used to assess the severity of the infringement. Finally, **paragraph 262** states that the ICO would also consider if issuing an enforcement notice if it "is likely to be:

56.1 effective in remedying the infringement; and
56.2 reasonable and proportionate in the circumstances of the case."

57 These factors and the ICO thought process they describe appears odd and irrational, for the reasons described above:

57.1 **Firstly**, an enforcement notice must, by definition, articulate steps to be taken to address an infringement of data protection legislation and bring processing into compliance. If an enforcement notice is not "effective in remedying the infringement", this would underscore an invalid, insufficient or baldy construed enforcement notice. It would not, however, reduce or subtract from the need to order an offender to comply with the legal obligations they should be following.

57.2 **Secondly**, enforcement notices are binding instructions given to ensure compliance with legal requirements that were mandatory to begin with. There cannot be a circumstance where an enforcement notice would not be "reasonable and proportionate", because there are no circumstances where the law does not apply to offenders.

57.3 **Thirdly**, enforcement notices are non-punitive regulatory action; thus, the severity of an infringement does not determine the content or appropriateness of an enforcement notice. Enforcement notices have only one degree of force, which is the force of law. Contrary to a penalty notice, whose amount can be increased or reduced according to the severity of an offence, an order to comply with the law cannot become more or less mandatory. Likewise, it would be irrational if the ICO were to ascertain an infringement of data protection law and then decide not to order the offender to comply, or to comply with some requirements but not with others.

Recommendations:

58 Guidance regarding the Commissioner's approach to issuing enforcement notices should be rewritten to reflect their role of effective remedy to an infringement of UK data protection role, and their suitability to prevent a repeated offence. This should, at a bare minimum, drop references to the gravity of the infringements as a reason to issue an enforcement notice, and make its issuing conditional to the existence of a breach of data protection law that needs be remedied or prevented from reoccurring.

59 The guidance should also state how the Commissioner would decide against the use of an enforcement notice and in favour of a different enforcement

remedy. Ideally, this would articulate why a legally binding order to comply with UK data protection law would not be necessary, and how the Commissioner would compare the effectiveness of these alternative responses against an enforcement notice.

11.2. Do you have any comments on the process for settlement discussions and concluding the case?

60 The description of the settlement procedure does not appear to make the validity of a settlement conditional on the controller or processor taking the steps they committed to during the settlement negotiation. We believe the guidance would benefit from stating in clear language that failing to implement the steps needed to comply with relevant provisions in the data protection legislation would cancel the "discount" provided for the settlement.

61 Further to this, t**he guidance states, at paragraph 350**, that a controller or processor would be required at a minimum to confirm that they will "take any steps needed to comply with relevant provisions in the data protection legislation or remedy the consequences of the infringement". This statement contradicts a previous statement of the guidance, according to which the controller or processor would be expected to "cease the infringing conduct immediately from the date it enters settlement discussions".

62 Also, this statement does not mention or suggest that such steps should be substantiated by any given deadline or timescale for being implemented. Such an "open ended" approach to settlement's commitments appears misguided, as it would leave the recipients of the settlement free to delay the implementation of these steps.

63 Finally, it is worth mentioning that certain controllers in the UK, for instance adtech providers, have a proven track record of abusing ICO engagement activities to delay enforcement by committing to take action that is never implemented in practice. The ICO approach to settlements would benefit from addressing this risk.

Recommendations:

64 The guidance should clearly state that the validity of a settlement is conditional to the recipient fulfilling their commitments.

65 The guidance should clearly state that the Commissioner should accept commitments during the settlement process only if they have a clear timescale against which their implementation can be assessed.

66 The guidance should clarify that failure to engage with the settlement process in good faith, or to implement the commitments taken during the settlement process, will invalidate the settlement, result in regulatory enforcement, and constitute an aggravating factor.

ABOUT YOU

Your name:

Mariano delli Santi

Email address:

mariano@openrightsgroup.org

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:

I am Legal and Policy Officer at, and I am responding on behalf of, Open Rights Group,