Submissions to the Information Commissioner's Office on the Consultation on its Draft Statutory Guidance

I. INTRODUCTION

The Centre for Information Policy Leadership (CIPL)[1] welcomes the opportunity to comment on the Information Commissioner's Office (ICO's) Consultation on its Draft Statutory Guidance (Draft Guidance) on how the ICO will exercise its data protection regulatory functions when issuing information notices, assessment notices, enforcement notices and penalty notices under the Data Protection Act 2018 (DPA) and General Data Protection Regulation (GDPR). We have a number of substantive comments that cannot adequately be conveyed using only the short-form survey that the ICO has created for this consultation. Accordingly, we have produced this short paper to supplement and explain our survey response.

The Draft Guidance states that it is intended to 'sit…alongside' the ICO's Regulatory Action Policy (RAP) and that '(t)aken together those documents set out how the ICO will support (its) mission (of)….uphold(ing) information rights for the UK public in the digital age'. The purpose of the Draft Guidance is to:

- provide clarity about the ICO's approach to statutory regulatory action, setting out a risk-based approach to enforcement by which the ICO will 'focus…on the areas of highest risk and most harm' to 'help create an environment within which data subjects are protected, while ensuring business is able to operate and innovate efficiently in the digital age'[2];
- 'maintain an effective and proportionate regulatory response', by setting out the nature of the ICO's statutory powers and being 'clear and consistent about when and how' they are used[3];
- discharge the ICO's statutory obligation to provide guidance as to how it proposes to exercise its functions in connection with information notices, assessment notices, enforcement notices, and penalty notices under Section 160 DPA.

CIPL welcomes the ICO's commitment to pursuing a risk-based approach to enforcement in order to safeguard individuals' rights, while enabling businesses to operate and innovate efficiently. CIPL also welcomes the ICO's commitment to ensuring an effective and proportionate regulatory response, which reflects a modern, strategic approach to regulatory engagement that achieves better outcomes for individuals, society and regulated organisations, while maximising the effectiveness of the

[1] CIPL is a global data privacy and cybersecurity think tank in the law firm of Hunton Andrews Kurth LLP and is financially supported by the law firm and over 85 member companies that are leaders in key sectors of the global economy. CIPL's mission is to engage in thought leadership and develop best practices that ensure both effective privacy protections and the responsible use of personal information in the modern information age. CIPL's work facilitates constructive engagement between business leaders, privacy and security professionals, regulators and policymakers around the world. For more information, please see CIPL's website at http://www.informationpolicycentre.com/. Nothing in this submission should be construed as representing the views of any individual CIPL member company or of the law firm of Hunton Andrews Kurth.

[2] ICO's Draft 'Statutory Guidance on our Regulatory Action', at 5.

[3] Ibid.

regulator[4]. However, there are several procedural and substantive points that we believe need addressing, in particular:

- The Draft Guidance appears to be largely a reproduction of relevant portions of the current RAP, save for the section at pages 19-24 which has been recast to describe an amended approach to calculating administrative penalties.
- Given that the RAP and the Draft Guidance are intrinsically linked, and that the current RAP is also being reviewed, the two documents should be available for consultation at the same time.
- It is not clear that the ICO's consultation process proactively includes many controllers and processors. Rather, reference is made to consulting 'ICO colleagues' and to conducting 'a formal consultation with the public'[5]. Section 160(9) of the DPA obliges the ICO to consult 'such other persons as the Commissioner considers appropriate', which should include those who will be most affected by the Draft Guidance. Industry bodies, groups representing controllers and processors, rights organisations and civil society should be proactively consulted on the substantive drafting of this document.
- The consultation itself is limited to soliciting very narrow responses to a limited range of questions. For such important guidance, forming a key part of the ICO's regulatory response, there should be a more detailed and open textured process, with a wider response pool and a longer timescale (especially at a busy time towards the end of the year, coinciding with several other consultations from the ICO and DCMS).
- The process that the ICO has detailed for the calculation of penalties sets out the wrong starting point for calculation, and also does not fully reflect the process described by the GDPR.
- There are areas in which more detail and clarity are needed, both in order to comply with the ICO's statutory obligations under the DPA and in order to ensure greater transparency.
- There is a missed opportunity for the ICO to build further on the RAP in the Draft Guidance and set out: a) a bolder vision and ambition of a modern, effective, proportionate, transparent and risk-based regulator, fit for a digital age in which there is great need to balance different fundamental rights and enable the responsible use of data in order to deliver benefits to society, the economy and people at large, and b) the progressive use of "nudge theory" of behavioral economics to encourage and reward positive behaviors and accountability (that goes beyond simple legal compliance), as well as robustly enforcing against deliberate or grossly negligent and repeated misconduct that creates real risks and harms to individuals.
- The Draft Guidance should refer and link to other ICO materials and initiatives, to ensure they are coherent and that they provide a unified message to organisations as to how they interact. In particular: a) how does participation in certifications and codes of conduct, demonstrating accountability, affect enforcement action and a potential statutory response, b) how would adherence to the ICO Accountability Toolkit be considered in the context of enforcement, and c) how would participation in an ICO Regulatory Sandbox impact on a possible subsequent enforcement action?

[4] See CIPL Discussion Paper: "*Regulating for Results: Strategies and Priorities for Leadership and Engagement*" and the article: "*Delivering Data Protection: Trust and Ethical Culture*" by Christopher Hodges

[5] Draft Guidance, page 6

II. CIPL COMMENTS

1. The Draft Guidance should clearly demonstrate the ICO's commitment to ensuring an effective and proportionate regulatory response, evidencing its risk-based approach, and emphasising the role of accountability

   - **The Draft Guidance should reflect more deeply the ICO's risk-based approach to enforcement:** The ICO has championed its risk-based approach to regulatory oversight and enforcement in numerous public statements, parliamentary hearings and other regulatory guidance (e.g. the RAP and its regulatory approach issued during the coronavirus pandemic[6]). The same approach should be reflected more deeply in the Draft Guidance and more explicitly in every enforcement action taken. While the Draft Guidance notes at the outset that it sets out the ICO's risk-based approach to taking regulatory action, this message does not generally permeate the detail of the Draft Guidance. Adopting a risk-based approach is beneficial to all parties, including the ICO, which will incur very high costs if it pursues punitive regulatory action against every organisation, without regard to the impact of the particular infringement and applicable circumstances.

   - **Accountability should be a strong mitigating factor when considering regulatory enforcement:** In exercising its statutory powers, the ICO should emphasise the role of accountability and organisational commitment to compliance, as well as behaviours that go beyond just legal compliance, as mitigating factors that will be considered following infringement. An assessment of accountability (from data protection management programs to formal certifications and adherence to codes of conduct) and best efforts to comply should be addressed explicitly as part of the ICO's risk-based approach. The ICO should actively encourage accountable behaviour from organisations by explaining how it will factor accountability into any assessment of infringement, and in determining an appropriate regulatory response, including the quantum of sanctions. There should be specific consideration of whether an organisation takes into account the ICO Accountability Toolkit in building and implementing its data protection management program. The Toolkit should be explicitly mentioned as one of the factors that may be taken into account in any enforcement action. Acts of non-compliance do not take place in a vacuum, and should be considered within the context of an organisation's wider data protection management program and any external certifications or adherence to a code of conduct. The same act of non-compliance should be evaluated differently by the ICO where an organisation has made every effort to implement and maintain an extensive data protection management program, compared with an organisation that has committed wilful acts of non-compliance. Further, the intent or good faith effort of an organisation should be a consideration when establishing the action that will be taken against it. For example, if an organisation has carried out a data protection impact assessment, considered the risks and attempted (in good faith but albeit unsuccessfully) to mitigate them, this should stand it in better stead than an organisation that has wilfully or negligently disregarded the existence of risk. Similarly, the level of oversight and supervision that senior management provides with respect to data management should be considered, as

[6] ICO's Updated Regulatory Approach in Response to Coronavirus

well as other elements of accountability, as advocated by the CIPL Accountability wheel and the ICO Accountability Toolkit.[7]

- **The ICO's proportionate approach to enforcement should be made clearer throughout the Draft Guidance without detracting from the level of clarity**: Generally, the Draft Guidance provides significantly more detail on the specifics of investigations, such as which documents may be requested by the ICO, where these documents might be accessed, and which staff might be interviewed, than it does with respect to the overall approach of the ICO. In particular, there is little information on how the ICO will exercise its judgment, or what a proportionate approach means in practice. Practical examples would be helpful.

- **The Draft Guidance should make clear how the ICO's enforcement approach relates to its regulatory objectives**: The rules set out in the Draft Guidance should be more explicitly tracked against the ICO's regulatory objectives, such as the protection of individuals and the promotion of transparency and proportionality in the handling of personal data. The benefit to data subjects of the ICO's adoption of a proportionate approach should also be emphasised. This will help organisations to understand the aims of the ICO with regard to its enforcement actions, enabling them to adjust their own approach to compliance so as to better meet the ICO's expectations (in addition to ensuring legal compliance). In this vein, we suggest that an additional factor for consideration in any decision to issue a notice referenced in this Draft Guidance should be the volume and nature of data subject complaints made in relation to an infringement, as this factor appears to be a consideration in other actions taken by the ICO, including those taken under the Privacy and Electronic Communications Regulations.

- **The Draft Guidance should include more information as to what will happen in the event of less serious infringement**: The Draft Guidance states that penalty notices will be reserved for the most serious infringement "in most cases". It is unclear how the ICO will exercise its enforcement powers or what penalties it will impose following less serious infringement. It would be helpful for organisations to understand whether such infringement will result in a smaller penalty, or no penalty at all, and to understand the nature of any alternative action that the ICO might choose to take. The ICO has the option to issue reprimands rather than penalties, although this is not made sufficiently clear in the Draft Guidance. It is essential that the Draft Guidance makes clear that there is a graduated spectrum of enforcement powers that the ICO can utilise, and that it sets out the criteria and organisational behaviours that will be taken into account in deciding where to draw the line on that spectrum. This would encourage organisations to build and implement the right controls and behaviours.

2. Some of the information that must be included in the Draft Guidance under the DPA is missing

- **Section 160 of the DPA sets out content that must be included in this Draft Guidance, some of which is currently missing**: For example, under Section 160 of the DPA, the ICO must provide the circumstances in which it will issue an "urgent" request. These circumstances are not clearly set out in the Draft Guidance. Under Section 160(4)(c)(i) the ICO must provide guidance as to the documents that are *not* to be examined under an assessment notice, and

[7] See CIPL Accountability Discussion Paper 1: "*The Case for Accountability: How it Enables Effective Data Protection and Trust in the Digital Society*"

this guidance is not currently included. In addition, the power of the ICO to cancel or vary its notices is not detailed in the Draft Guidance. Organisations should be informed of this so that they understand that there will be instances in which organisations and the ICO can cooperate and solve issues early on in the process, without resorting to enforcement. This would encourage organisations to be more cooperative and transparent.

- **The statutory obligations that the ICO is subject to are not made clear in the Draft Guidance**: For example, in relation to the provision of a notice of intent to levy a penalty against an organisation, the Draft Guidance does not make clear that this is required by law[8]. In addition, the instances in which the ICO may *not* issue notices, such as assessment notices under Section 147 DPA, should be detailed. These obligations should be made explicit so that oragnisations have a complete picture of how the ICO will exercise its statutory powers.

3. Limitations on the ICO's power are unclear, particularly with respect to the documents it may access

- **Access to privileged material**: Section 133 of the DPA requires the ICO to provide guidance on this issue, including how the ICO will ensure that such materials are used or disclosed only insofar as is necessary for carrying out the ICO's functions, and how the ICO will comply with restrictions and prohibitions on obtaining or having access to privileged communications which are imposed by an enactment. In particular, Section 143(3) and (4) of the DPA states that an information notice does not require the disclosure of material which would be privileged, and there is a similar provision in relation to assessment notices (see Section 147(2) and (3)). These restrictions are not mentioned in the Draft Guidance which instead contains unclear statements as to the ICO's ability to access all information it requests, referring to the Attorney General's guidelines on disclosure as governing how it will handle material that may be subject to legal professional privilege. Given that the Attorney General's guidelines were drafted in 2013, in a different context, we suggest that more detailed, tailored and up-to-date guidance is required from the ICO in the Draft Guidance itself. More clarity should be provided as to the safeguards that will be implemented to determine whether privileged documents are relevant, the process for verifying whether privilege arises, specific safeguards to enable the ICO to review the documents, safeguards to ensure that the organisation entitled to assert privilege is not subsequently disadvantaged by having disclosed privileged material to the ICO, and a process for resolving any disputes about these matters.

  If access to legally privileged information or commercially sensitive information is to be requested, organisations should be given some indication of when such access is likely to be requested and the approach of the ICO when determining whether or not such access is necessary, given the potential disruption and concern this may cause. In addition, the rights that the organisation may have to withhold such information should be fully explained (at present the draft simply refers to "other access conditions" that the organisation may request with respect to certain information to be reviewed by the ICO).

[8] Schedule 16 DPA

4. The proposed nine step process for calculating administrative penalties is cumbersome and overlapping, apparently focussing on an organisation's turnover rather than on the harm caused by the infringement, and the culpability of the organisation

- **The calculation of penalties should be undertaken on a case-by-case basis, without the use of pre-determined figures or percentages:** The Draft Guidance states that the ICO will assess each case objectively on the facts with respect to penalty notices. This evaluative and pragmatic approach should be applied clearly and more widely to all of the action taken (or not taken) under this Draft Guidance, reflecting the unique nature of each organisation, its resources, the extent of its data protection compliance program, the nature of its data handling activities, etc. The calculation of penalties should not commence with establishing the upper limit, which ignores the specific nature of the infringement at hand. Whether an infringement falls into the higher tier of penalties under Article 83(5) or the lower tier of penalties under Article 83(4) should not frame the ICO's calculation of a penalty, which should be based solely on the seriousness and nature of the infringement itself, and the organisation's culpability. Article 83 provides statutory limitations on the amount that an organisation may be fined, and is therefore indicative of the seriousness with which breaches of different Articles should be treated. However, these amounts are not meant to form the starting point for a calculation.

- **Assigning a set percentage figure based on only three possible categories is a crude measure of culpability**: Assigning a percentage figure to negligent or intentional acts fails to recognise the scale of culpability that exists. Not all negligent acts are equally negligent, for example. The ICO should approach the imposition of penalties by assessing a range of factors holistically and in combination with one another, using its expertise and experience to judge the severity of an infringement. A simplistic, formulaic approach would not permit the ICO to exercise its judgment appropriately. In addition, the table provided on page 23 of the Draft Guidance suggests that penalties will be imposed even where there is no culpability on the part of the organisation. This position should be clarified. The ICO has made clear in penalty notices issued under the GDPR that an organisation will remain culpable in the event that it suffers a cyber-attack, if it failed to take reasonable and appropriate measures to prevent such an attack. However, if the organisation is not culpable at all, having taken all appropriate measures to prevent an infringement, it should not be subject to a penalty.

- **Turnover is not an appropriate measure of culpability and should not be the starting point for calculating a penalty:** The decision as to whether to impose a penalty is the starting point, followed by consideration of the size of the penalty. While turnover is relevant to establishing the upper limit of a penalty, penalties should not be proportionately increased based purely on the higher turnover of an organisation. Turnover may be a relevant factor where the breach or infringement in question has allowed the organisation to make financial gains, but in many instances infringements do not result in gain. For example, if a breach relates to the data of an organisation's employees, it is not clear why the organisation's turnover would have any relevance to establishing a starting point for the calculation of a penalty. In addition, turnover is not a suitable measure to use in calculations for all organisations - for example it will not be appropriate for non-profits.

- **The Draft Guidance should set out all factors considered in the calculation of a penalty**: As regards penalty notices, the Draft Guidance lists a number of factors that will be considered when establishing whether a penalty notice is to be served, and if so the amount of any penalty. However, the mandatory factors for consideration set out under Section 155(3) of the DPA and Articles 82(1) and (2) of the GDPR are not listed exhaustively. Factors that are missing from the Draft Guidance include the number of data subjects affected by an infringement and the degree of damage suffered. In addition, the assessment of the culpability of the organisation, and the intentional or negligent nature of the organisation's failings are then assessed as part of "Step 2" of the calculation of a penalty, when in fact these are the considerations that should form part of the list described in "Step 1", not a separate stage in the process. As currently drafted, this provides incomplete information to the organisations the ICO seeks to regulate, some of which may not be familiar with the detail of the relevant legal provisions.

- **Alternative approach to calculating penalties:** We propose the following simpler alternative process for calculating penalties:
  - The first stage should be an assessment of whether or not, given the circumstances of an infringement and the factors listed under Article 83(2) of the GDPR and Section 155(3) of the DPA, a penalty should be imposed, or other action (such as a reprimand or enforcement notice) should be taken.
  - If a penalty is to be imposed, there should be an assessment of the nature and seriousness of the matter to determine whether the infringement falls under Article 83(4) or (5), in order to establish the relevant limit of a penalty (i.e., whether the penalty falls into the upper 4% bracket, or the lower 2% bracket).
  - Next, there should be an assessment of mitigating or aggravating factors, in particular taking into account the implementation of accountability tools and the level of culpability of third parties (such as hackers). There should be no calculation before these factors are considered, as they go to the seriousness of a breach.
  - The fourth stage is to set the penalty, taking into account whether the organisation is an "undertaking" and, if so, whether turnover is relevant to the infringement. The assessment should also consider the relevant geographic area in which the infringement occurred, the nature of the infringement, any gain to the entity, and the value of any gain.
  - The final stage would include consideration of the financial means of an organisation and the economic impact of a penalty. These should be part of the same assessment, rather than taking place in two stages as suggested in the Draft Guidance.

  A penalty reduction for early payment should not be considered as part of the calculation of a penalty itself. It is a reduction that is separate to an assessment of the seriousness of a breach or mitigating factors, and is essentially administrative and unconnected to the relevant infringement. This should be made clear by removing it from the calculation section of the Draft Guidance.

- **The Draft Guidance should clarify the role of 'other Concerned Supervisory Authorities' in setting the final amount of any penalty:** The Draft Guidance refers to the ICO considering representations from 'other Concerned Supervisory Authorities' when setting the final

amount of a penalty[9]. There is no reference to any process by which the controller or processor would be informed of such representations, or any indication of what information would be shared with Concerned Supervisory Authorities. The ICO's website states that the Draft Guidance will be published after the UK 'has left the EU'. However, after the end of the Brexit implementation period, i.e. from January 1, 2021, no other Concerned Supervisory Authorities will exist with regard to penalties imposed by the ICO, or the exercise of any other regulatory power. These points should all be clarified.

5. Given the significance of the issues addressed in this Draft Guidance, which go to the core of the ICO's enforcement strategy, data controllers and processors are key stakeholders and should be specifically targeted as part of the consultation

   - **Data controllers and processors have not been specifically consulted:** In preparing the Draft Guidance, the ICO has consulted 'ICO colleagues' and is conducting 'a formal consultation with the public'[10]. Section 160(9) of the DPA obliges the ICO to consult 'such other persons as the Commissioner considers appropriate', which should include those who will be most affected by the Draft Guidance. As the ICO has done for other significant guidance, it should consult widely in preparing this Draft Guidance, including industry bodies, groups representing controllers and processors, rights organisations and civil society as key stakeholders. Our informal soundings suggest that there is minimal awareness of this particular consultation. Recent enforcement action by the ICO indicates that (unsurprisingly) organisations will closely evaluate and challenge the ICO's enforcement strategy and guidance. Given this, the ICO may wish to consider engaging proactively with organisations on some of these issues. We propose that more detailed and collaborative consultation is carried out with controllers and processors that will be affected by the Draft Guidance.

6. Clarity is needed as to how the Draft Guidance will interact with other ICO policy and guidance documents

   - **The relationship between the Draft Guidance and the RAP should be clarified and the two documents reviewed and updated together**: The Draft Guidance states that the RAP is currently under review. The RAP sets out the ICO's approach to taking enforcement action across all of the areas that the ICO regulates, including data protection. The Draft Guidance explains how the ICO will exercise its functions in connection with information notices, assessment notices, enforcement notices and penalty notices, and appears to be largely a reproduction of relevant portions of the current RAP (save for the section at pages 19-24 which has been recast to describe an amended approach to calculating administrative penalties). Clearly the two documents are intrinsically linked and they should be available for consultation and discussion with stakeholders at the same time. They should be read together and refer to each other. This would assist organisations in understanding precisely the ICO's policy and intention, the behaviour that the ICO expects of them, and the nature of the enforcement action to which they may be subject.

   - **The Draft Guidance should identify the document it is designed to update/replace and make clear the time period from which it will apply:** There is no specific reference in the Draft

[9] Draft Guidance, page 19
[10] Ibid, 6

Guidance to the previous version, or from which date this new version will apply. Section 160(8) DPA permits the ICO to produce altered or replacement guidance. The Draft Guidance states that it: "contains all guidance on the ICO's approach to the use of our regulatory powers that we have a statutory obligation to provide under the DPA 2018"[11]. This appears to mean that no statements in earlier guidance or statements in other ICO materials, such as the general guide to the GDPR, will be taken into account in considering regulatory activity covered by this Draft Guidance. If this is the case, there should be a clear statement that this is replacement guidance, and clarification of whether this document replaces all prior material produced by the ICO on the subject of these powers or only the prior version of this particular document (which is not identified but which appears to us to be part of the current version of the RAP). All other ICO material that refers to these powers should explicitly reference this Draft Guidance, and other relevant material, such as the RAP, to demonstrate a holistic, consistent approach by the ICO.

- **Apparent overlap with other regulators and regulatory supervision should be clarified:** The introduction to the Draft Guide refers to joint working with others - "We will work with others where it makes sense to do so, and where joint application of activity can achieve the best result and protection"[12]. Overlap with other regulators and regulatory supervision will be an important interface for many businesses, such as in the financial services sector, in relation to competition law and consumer protection law, or in respect of forthcoming online harms regulation. This overlap and convergence of different regulators is only going to increase with the growth of the digital economy and data use in all sectors. The Draft Guidance should either clarify how this overlap or joint activity will be approached, or refer to other materials such as memoranda of understanding or the work that the ICO has commenced with respect to Regulatory Hubs and the Regulatory Sandbox. The current statement is not an appropriately clear or transparent statement of policy in this area. It does not identify which other bodies the ICO will work with, how they will work together, whether the ICO will take the lead or defer to other regulators, or where and how those arrangements will be set out so controllers and processors can see them.

7. <u>Sections of the Draft Guidance lack detail and clarity that would assist organisations and aid transparency</u>

- **The extent of the ICO's discretion, and how it will be exercised, should be made clear:** The Draft Guidance makes reference to the issuance of notices when the ICO considers it "necessary" and at its "discretion" [13]. While the ICO has a degree of discretion, there are specific statutory obligations with which organiations are required to comply, and it is non-compliance or suspected non-compliance with these obligations that should trigger action by the ICO, not the ICO's judgment alone. What may trigger the issuance of an information notice is not made clear in the Draft Guidance. For example, is an information notice likely to be issued following a breach? Following a consumer complaint or a tip-off from a third party? Following an inquiry from the organisation itself on a data protection matter? This latter question is important, as some organisations may avoid seeking information or advice on data protection issues from the ICO if they believe that a query might spark a regulatory inquiry. It

[11] Draft Guidance, page 6
[12] Ibid, 5
[13] Ibid, 8

is also not clear whether an information notice will only be issued in the event that the ICO suspects there has been an infringement of data protection law, or in other circumstances. Section 142(1) of the DPA provides that an information notice may be issued to require an organisation to provide the ICO with the information it "reasonably requires" for the purposes of carrying its functions under data protection legislation, but organisations would be assisted if the ICO could provide some concrete examples or criteria for when such a need would be likely to arise. The ICO must also set out in the notice the basis on which it is given and why the ICO requires the information.

Conversely, there are also instances where the ICO implies that it does not have any discretion at all, such as when setting the amount of any penalty in the context of its regulatory work.[14] However, the ICO does have discretion on these matters, and any language that suggests otherwise and confuses this issue should be clarified or removed from the Draft Guidance.

- **The relative weight of each factor the ICO will take into account when considering penalties should be made clear**: More clarity should also be provided as to the weight to be attached to each of the factors listed by the ICO that may result in a penalty being imposed,[15] and whether they are considered in isolation or conjunction with one another. The relative weight of each may depend on the unique nature of each breach, but to the extent that certain factors are likely to be determinative of whether or not a penalty is imposed or is likely to increase, these should be highlighted.

- **The ICO's process for enforcement should be made clear**: The Draft Guidance refers to options the ICO will have in certain circumstances, such as the further action that may be taken where an enforcement notice is not complied with.[16] Transparency requires that all of the options that are available to the ICO should be set out, so that organisations may understand the full range of possibilities. With regard to enforcement notices specifically, Section 160(6)(c) requires that the ICO provide information as to how it will proceed if a notice is not complied with. The DPA also requires that certain content be provided in information notices, including the specific ground on which it is served. It should be made clear to organisations that certain decisions will be taken only in certain circumstances or if certain thresholds are met, and certain criteria fulfilled. These thresholds and criteria should be clearly detailed in the Draft Guidance, so that organisations are aware of the type of behaviour that is likely to trigger enforcement action from the ICO. Finally, the Draft Guidance should make clear that the burden of proof with respect to any relevant breach of data protection law lies with the ICO, and that the ICO will also bear the burden of justifying any action it takes.

- **The Draft Guidance contains inaccurate drafting inconsistent with the law:** There are instances where the Draft Guidance uses language that is not consistent with the law. For example, the Draft Guidance refers to giving an information notice to an 'individual'. This reference should be to a "person"[17], which would include a legal person, since such notices may be given to organisations (legal persons) as well as to individuals. As a further example, in respect of enforcement notices, it is stated that the ICO may serve an enforcement notice where processing or a transfer to a third country fails or "risks failing" to meet the

[14] Draft Guidance, page 20
[15] Ibid, 18
[16] Ibid, 17
[17] See s.142(1)(b) DPA

requirements of data protection legislation[18]. In our view this does not reflect the law, under which the ICO must be satisfied that 'a person has failed, or is failing' to comply[19]. It is not sufficient that a failure may occur in the future[20].

- **The structure and language of the Draft Guidance should be consistent and clear**: There is inconsistency between different sections of the Draft Guidance, which may disadvantage an uninformed reader. To ensure clarity and transparency, the same material should be reproduced with respect to each type of notice, preferably with the same set of headings. For example, rights of appeal, or the formalities with respect to each type of notice should be clearly set out. Currently, the section on enforcement notices lists what the notice will contain, and includes a reference to the appeal process[21]. In contrast, the sections dealing with information notices[22] and assessment notices[23] do not mention rights of appeal at all, despite the availability of such rights in respect of both types of notice. Each section should also fully explain the rights of organisations, and the exemptions or limitations that may apply[24].

  In addition, some statements appear contradictory. For example, with regard to assessment notices, the Draft Guidance states: "We will access the minimum amount of information we need to assess whether the organisation is handling personal data appropriately"[25]. A few sentences later, it states: "Organisations can contact us to request that, if an assessment notice requires access to such information, this access is limited to the minimum required to adequately assess their compliance with the legislation." This suggests an organisation must actively request that access is limited, and it is not clear whether an organisation will be told of the ability to request a limitation on access to certain types of material.

8. <u>There are several additional points that should be included in the Draft Guidance</u>

- **The Draft Guidance should clarify when a penalty is considered 'significant', requiring that a panel of non-executive advisers will be convened:** The Draft Guidance refers to the convening of a panel comprising non-executive advisers to the ICO when significant penalties are under consideration[26]. This is certainly a good and innovative practice that should be encouraged. However, it is not clear what will constitute a "significant" penalty (although the current RAP states that these are 'expected to be those over the threshold of £1M').

---

[18] Draft Guidance, page 16
[19] See s. 149(1) DPA
[20] A third example is also offered. The Draft Guidance states that assessment notices can be issued for material which is subject to national security certificates. No authority is cited for this. However national security certificates issued under s.26(e)(ii) DPA cover all the Article 58 GDPR powers. S.115(6) states that the ICO can only exercise her powers under Article 58(1)(b) to carry out audits in accordance with s.146. In serving an assessment notice under s.146 the ICO is exercising a power under Article 58. Accordingly, it appears that the ICO cannot serve an assessment notice in respect of material covered by a national security certificate. The reference in the same paragraph to Section 23 of the Freedom of Information Act is therefore also odd as such information could be covered by a national security certificate. In addition the ICO cannot serve notices on the security services where an exemption is required for the purposes of national security s.110(2)(e).
[21] Draft Guidance, page 16
[22] Ibid, 8
[23] Ibid, 10
[24] See Sections 142(4)(b) and 146(5)(b) DPA
[25] Draft Guidance, page 12
[26] Ibid, 19

Additional information should also be provided on when such panels are likely to be convened, and the parties most likely to serve on them. For example, whose interests would such parties represent? What will be the qualifying criteria for sitting on such panels? Would organisations have the ability to make representations to the panel?

- **The Draft Guidance should go further in explaining when certain notices will be served, and on whom, distinguishing between controllers and processors:** The guidance as currently drafted states that it is designed to inform controllers and processors about the statutory powers of the ICO[27], but does not provide clarity as to when enforcement action will be taken against a controller or a processor. For example, it is not clear whether processors may only expect information or assessment notices with respect to their own data processing practices, or whether they may also receive such notices from the ICO in the event that an investigation of the data practices of the controllers on whose behalf they are carrying out processing is conducted.

- **Illustrative examples of the behaviour** most likely to trigger certain actions from the ICO would be of assistance to organisations.

- We suggest that the **conduct of an organisation** in response to a notice issued by the ICO only be considered a relevant factor where it is markedly above or below the legal obligations organisations are under. This should be made explicit in the Draft Guidance.

If you would like to discuss any of the comments in this paper or require additional information, please contact Bojana Bellamy, bbellamy@huntonAK.com; Bridget Treacy (btreacy@hunton.com); and Olivia Lee (olee@hunton.com).

[27] Ibid, 6

Appendix: Minor Clarifications/Updates Required

In the table below we have provided an overview of the minor clarifications and updates that we recommend implementing in the final update of the Draft Guidance.

Assessment notices	
When will we issue an assessment notice?	
Page 10	Bullet point 3 refers to reports which "suggest" there is non-compliance. This should be clarified with regard to the importance of the level of credibility of the source or the seriousness of the allegations.
Enforcement notices	
When will we issue an enforcement notice?	
Page 16	Bullet points one and two, setting out when enforcement notices may be issued, appear to overlap – we recommend amalgamating these points. The Draft Guidance states: "When deciding whether to issue an enforcement notice, we will consider the factors set out above, including whether there are any mitigating or aggravating factors". It is unclear which factors are referred to here.
Penalty notices	
Page 17	The Draft Guidance states that a penalty notice indicates the ICO's intention to impose a penalty. In fact, it is the mechanism by which the ICO *actually* imposes a penalty. It is distinct from a notice of intent, but some readers may not be aware of the distinction.
When will a penalty notice be appropriate?	
Page 18	The Draft Guidance provides an indicative list of factors that may result in a penalty being imposed, this is currently drafted as cumulative ("and" rather than "or") – we assume that in reality these are separate factors, each of which would be considered as making a penalty more likely.
What will be the amount of any penalty?	
Page 20	The Draft Guidance refers to an "undertaking", but there is no explanation of the meaning of this phrasing, and no reference to how parent companies or local subsidiaries will be treated under the Draft Guidance. We suggest providing links to other ICO guidance and materials that will provide clarity on these kinds of phrases, if definitions are not to be provided within the Draft Guidance itself.
General Clarifications	
Page 7	Bullet points one and five overlap and are duplicative – we recommend amalgamating these points. Bullet point nine refers to "administering" a penalty. This should instead refer to "imposing" a penalty.
Page 8	A "suite" of guidance is referred to. This implied there are additional resources separate from this document. We recommend referring to a "range of support".