Summary of responses from the statutory guidance public consultation (October 2020)

Summary of responses

Introduction

In October 2020, the ICO published its draft Statutory Guidance on how it will exercise its data protection regulatory functions of information notices, assessment notices, enforcement notices and penalty notices. The ICO is required under the Data Protection Act 2018 (DPA 2018) to produce the Statutory guidance and as part of this process consult externally on its content before formally submitting the final guidance to the Secretary of State for Digital, Culture, Media & Sport for tabling for Parliamentary approval.

The external consultation commenced on 31 October 2020 with the deadline for comments Thursday 12 November 2020. The survey asked for views on:

- the clarity and presentation of the guidance;
- any further guidance or information that would be helpful for organisations;
- practical examples of any further information that could further help organisations or organisations understand how the ICO will exercise its functions; and
- provided an opportunity for respondents to make any further general comments.

The consultation ran for a period of six weeks. In total, we received 58 responses to the consultation. Of these, 55 responded via the survey. The three remaining responses were received by email correspondence. Reassuringly, there was a large amount of positive feedback on the scope and structure of the guidance with 89% of respondents[1] stating that the guidance was extremely, very, or moderately useful. Having taken these responses into consideration, they have provided us with useful insight as to where we could make improvements. In particular, we received useful responses regarding where additional resources for DPOs, organisations and the public would be helpful, with many suggestions received about how we could support DPOs and the potential value practical case study examples could bring in facilitating understanding of the ICO's 'risk based approach'.

It is clear that there is a desire for greater clarity around how the Statutory Guidance will interact with the updated Regulatory Action Policy, this feedback has been invaluable as we continue to develop the RAP for public consultation. The RAP will aim to set out the responsibilities we have and how we will use the actions we take to encourage organisations to comply with the laws we monitor and enforce. The RAP focuses on the range of legislative

[1] Based on 53 responses to the survey question 'are these sections clear and easy to understand?'

provisions we deal with outside of our compulsory statutory obligations, which are dealt with by the Statutory Guidance, thus bridging the gap and bringing together the two documents into one single set of guidance.

The ICO would like to thank all those organisations and individuals who took the time to read the draft guidance and give us their views, and those who offered to work with us further. We are especially grateful that even in times of a global pandemic, you made time to engage with us on this guidance. We have carefully noted all the comments received, and these have been invaluable in shaping our thinking on the final version of this guidance and our Regulatory Action Policy.

While we cannot respond individually to each contribution, we have provided an overview below of the key themes that have become apparent and some comments on our emerging thinking from each area.

For this consultation, we are publishing all responses we receive, unless it was requested otherwise in the survey. For the responses we publish, we will remove personal contact details.

Themes

Clarity & presentation

Many respondents felt the draft Statutory Guidance is clear and easy to understand, with comments like it is well-written, logical and clearly set out.

However, some respondents commented that it needed more clarity, although often this seemed to overlap with wanting more detail in the text, with further explanations (see the theme 'Granularity of detail').

Some noted a few typographical errors. As an example, on the 'Penalty starting point' table on page 23, the highest percentage of fine only goes up to 3% and not 4%. A query was raised whether this was an error. Another example is 'processer' instead of 'processor' on page 6. Others suggested some changes to certain phrasings to aid clarity, such as changing 'standard maximum amount' and 'higher maximum amount' to 'standard penalty breaches' and 'higher penalty breaches'.

In addition, to further aid clarity, some suggested adding in several 'real life' examples to illustrate the points being made, or situations where the ICO may take certain types of regulatory action. Again, this links with the 'Granularity of detail' theme.

A further suggestion was to add a flow chart to the first section of the draft Statutory Guidance to demonstrate the regulatory action covered as it increases in intensity. Another was to be more consistent with, and better explain, the links to further reading materials.

Another point raised was that there should be greater consistency between the content of each section of the draft Statutory Guidance covering the different types of notices that can

be issued. This means each section should include the same format, preferably with the same set of headings, covering the same sort of details, such as process of issuing a notice, any right of appeal and so on. It was suggested this would ensure clarity and transparency in the text.

There was some uncertainty about the meaning of some of the terminology used, such as defining what 'statutory status' means, the difference between an assessment notice and an audit, references to certification, and the use of 'Euros' in the context of the UK exiting the European Union. It would be helpful to explain some of these terms.

A few respondents noted that the draft Statutory Guidance appears to be aimed at data protection professionals, even though the audience includes members of the general public. It was suggested by one respondent that a summary or overview document to accompany the draft Statutory Guidance would be useful. Another suggested some minor formatting changes to perhaps aid non-practitioners, such as by using more bullet points. There was also a suggestion of creating a simpler version of the Statutory Guidance – including a child-friendly one.

Some respondents commented on more general aspects of the draft Statutory Guidance, which also link with the other themes discussed below. In particular, some expressed the view that the draft Statutory Guidance takes a high-level and strategic approach, with not enough detail, making it difficult to understand what will guide the ICO's regulatory decision making in practice. This could leave the average person not much clearer about when it will act. There was a related call for the Statutory Guidance to be less vague and more definite, rather than sometimes making some general statements about what the ICO may or may not do.

Similarly, some felt there was not enough clarity about how the ICO will exercise its regulatory powers and how it will decide to intervene in cases, or what organisations it will prioritise for regulatory intervention. Others suggested there was a focus on big data breaches, high profile cases, but not how the ICO will look at the poor practices of organisations that impact on the rights of individuals, with a concern that certain groups may not be high on the ICO's list of regulatory priorities.

Consequently, some felt the draft Statutory Guidance potentially needed to be supplemented by a second set of guidance or instead further developed. (Again, see 'Granularity of detail').

Relationship with the Regulatory Action Policy

A key theme that emerged concerned how the draft Statutory Guidance relates to the ICO's Regulatory Action Policy (RAP).

A number of respondents queried the relationship of draft Statutory Guidance with the RAP, noting the two are linked, yet the latter is still under review. Some felt it would have been more beneficial for both sets of documents to have been consulted on at the same time and also to cross-reference each other. Some felt there was some uncertainty with how both the

Statutory Guidance and the RAP interact going forward. Linked with this, some respondents noted that the draft Statutory Guidance states it contains all the guidance on the ICO's approach to the use of its regulatory powers that it has a statutory obligation to provide. However, they were uncertain how the Statutory Guidance interacts with the RAP, last published in 2018, which stated it was aimed at fulfilling this same statutory obligation. They felt that further clarification is needed about how the RAP currently under review and the draft Statutory Guidance join up.

Others also commented that the Statutory Guidance should identify what it is designed to update or replace and also to make clear the period from which it will apply. There was some concern that the wording of the Statutory Guidance suggests that no statements made by the ICO in its earlier guidance or in other ICO materials will be taken into account when considering regulatory activity. This should be clear if this is the case. The question was therefore raised whether the Statutory Guidance replaces these other statements or only prior versions of the document it is intended to replace. Furthermore, it was noted that the Statutory Guidance and all other ICO materials or policy statements that refer to the ICO's regulatory role should be aligned and refer to each other for a holistic, consistent approach.

Consequently, some respondents thought the relationship between Statutory Guidance and the RAP needs to be made clearer, not just in their scope but also in their nature. It should be highlighted what is outside the scope of the Statutory Guidance but within the scope of the RAP.

In terms of comments more specific to the Statutory Guidance, a question was raised about why the matters covered by sections 133, 158 and 160 of the DPA 2018 are covered in one single document, when the guidance required by section 160 is subject to a more specific parliamentary approval procedure.

A few respondents queried whether other data protection considerations should be included within the Statutory Guidance, such as how an organisation's participation in the ICO Sandbox, or adherence to the ICO's Accountability Framework would be taken into account when deciding on regulatory action. There was also a suggestion that the ICO should have regard to whether an organisation has received certification under the GDPR or its adherence to a code of conduct when making decisions about using its statutory powers.

Enforcement factors

Some respondents felt there was a lack of clarity in the Statutory Guidance about when the ICO will take regulatory action and that the focus is more about processes for issuing various types of notices. They thought it was difficult to know what will guide the ICO's decision making process in practice.

Others felt the ICO doesn't take enough enforcement action and provided comments that it should do more, and to better reflect this in the Statutory Guidance. Comments ranged from the view that the ICO has shown itself to be unwilling or unable to effectively enforce the law, or failing to adequately police the GDPR, with others commenting that the ICO should be serving many more penalty notices, even when only one individual has been affected. This is

linked to a similar point that a penalty notice should be appropriate when one individual has been severely affected, not just when lots of individuals have been affected by a contravention. Still, other respondents felt that the ICO should look at lower-level issues to detect more systemic and deep-rooted problems that can affect vulnerable groups in particular. Similarly, some were unclear how the ICO will use its powers or what penalties it will impose for less serious infringements.

Linked to this was the comment that the ICO's enforcement action seems to be focussed on big data breaches, high profile case, or where individuals with power to press for intervention are affected. It does not seem to look at the lower level poor practice in an organisation which can adversely impact on the rights of individuals. Similarly, another felt that the ICO seems to only take action against organisations whose non-compliance affects large numbers of people rather than individuals, even though the legislation confirms that each individual has rights that should be protected.

There was a suggestion that the ICO's regulatory approach needs re-balancing between being a 'regulatory consultant' and a 'regulatory enforcer'; the ICO doesn't do the former very well, and needs to demonstrate more of the latter.

A concern that was expressed about the ICO's perceived approach to regulatory action is that DPOs who identify risks or compliance issues within their organisations are too easily ignored by their management, as there seems to be a low likelihood of regulatory action being taken. There were calls for more support for DPOs in that the ICO should be actively supporting them so they aren't penalised (by their employers) for carrying out their jobs and acting where this takes place. Similarly, a query was raised whether the fact an organisation has taken notice of its DPO's advice is a factor to be taken into account when deciding what action to take.

Some questioned why the ICO appears to be concerned in the Statutory Guidance with ensuring that commercial enterprise is not constrained by red tape or concern that sanctions will be used disproportionately. They noted the ICO's duty is to supervise the fundamental right to the protection of personal data. It should therefore commit to protecting the rights of UK data subjects to the same extent as those in the rest of EU. The starting point for most egregious contraventions should be the maximum fines available and there should be a commitment to using penalties in the same way as other supervisory authorities. A measure of this could be by benchmarking the ICO against supervisory authorities in other EU countries.

Others thought the Statutory Guidance should make clear the aggravating factors that will be taken into account when determining what action to take. They felt that sometimes organisations may have taken advantage of the ICO's regulatory approach as more of an 'educator' in order to avoid or delay enforcement action. As a consequence, they were of the view that should an organisation fail to comply with a notice or with their own commitments to improve their practices, the ICO should take these aggravating factors into account and apply stronger sanctions when determining what action to take.

A few commented that they would like to see the ICO have stronger powers, including making individuals within an organisation personally liable, or making certain infringements a criminal offence. Also, a suggestion was made that certain types of notices, such as an Assessment Notice, should be mandatory wherever an infringement has occurred.

Some respondents cautioned against the unintended consequences of regulatory action by the ICO. In particular, that fining an organisation can be counterproductive to the individuals who use its services, such as a healthcare body which would have to divert funds away from patients to pay the fine, or other providers who would otherwise have less money to pay for their clients.

A comment was received that the Statutory Guidance states the ICO may serve an Enforcement Notice where the processing or transfer to a third country fails or 'risks failing' to meet data protection requirements. However, they felt this was inaccurate, and that the ICO must be satisfied that a person has failed, or is failing to comply, rather than merely that a failure may occur in the future.

A query was received about the extent of the ICO's powers and suggested there seems to be no power to issue a 'cease activity' order.

Other respondents wanted to see the inclusion in the Statutory Guidance reference to certification, which could be beneficial to regulatory activity. They thought this would also bring the Statutory Guidance more in line with the Regulators' Code, in that when assessing risks, the regulator should recognise an organisation's compliance history, including the use of earned recognition and evidence of relevant external verification. In that light, certification should be taking into account when deciding what regulatory action to take.

There was a suggestion of creating a publicly accessible database of ICO enforcement action, which could help with transparency, beyond highly publicised major breaches.

A comment was that the ICO should make it clear what kind of investigation is being undertaken from the beginning, and to advise organisations that they should consider legal representation to ensure their Article 6 ECHR rights are protected. However, it's less clear how this applies to the draft Statutory Guidance.

Granularity of detail

There was a great deal of feedback concerning the level of detail provided by the draft Statutory Guidance, ranging from general comment to more specific sections.

General feedback

There were several calls for greater clarity and detail on the information provided. Some respondents felt parts of the Statutory Guidance were vague and lacking in detail to be really useful. Some thought the draft Statutory Guidance was very high-level, and often respondents wanted more examples to illustrate both the general processes and the points being explained. For example, the Statutory Guidance ought to show in more specific detail the factors that will influence the ICO's regulatory intervention.

Some respondents suggested the ICO can exercise a lot of latitude in terms of its regulatory decisions, so more detail is needed in the Statutory Guidance to aid transparency, and they felt the text currently doesn't add much to what is already known.

Other details respondents would like to see more of include practical examples of mitigating and aggravating factors; how best or poor practice impact enforcement action; as well as the timescales for different actions.

In terms of notices, they also wanted to know whether the steps taken to issue a notice come sequentially or is there scope to go straight to enforcement. Furthermore, what the thresholds for issuing notices are; the procedural rules and processes applied; and whether draft or preliminary notices will be circulated to organisations first. Respondents also wanted to know how the ICO will deal with delays in responding to notices due to complex issues or the scope of a notice being unclear, as well as how to appeal notices. Some felt it would be useful to detail the ICO's power to cancel or vary its notices, so they can understand there will be instances where both the ICO and the organisation can cooperate and solve issues early without resorting to enforcement.

Some wanted more details on what types of information or records the ICO would expect to have access to as part of its regulatory activities, emphasising the need for organisations to understand their data ecosystems to satisfy this.

Some respondents queried how the ICO will engage and work with other regulators as suggested by the introduction to the Statutory Guidance.

Some wanted more detail about the 'Evaluation and next steps' section, although another respondent questioned the usefulness of this section of the Statutory Guidance as not adding any value and suggested its removal. One respondent requested sector-specific guidance.

There was a comment that the Statutory Guidance should make clear that it doesn't cover criminal prosecution powers, whereas a related comment is that the Statutory Guidance should clarify the distinction between personal data obtained for a civil matter and a criminal act.

Some queried how the ICO will assess the effectiveness of its regulatory action.

Information Notices

Respondents called for more detail on the thresholds for issuing an Information Notice, including examples. They would like to see examples that include triggers for issuing the notice, what information may be requested, and how long organisations have to respond and whether this can vary. Others requested more detail on the factors considered, such as types and level of risk of harm, or distress caused, and the methodology for determining this. Some felt the public interest aspect is unclear and open to interpretation.

Others wanted further clarification on the extent of the ICO's discretion in issuing an Information Notice and how this will be exercised, with the criteria used and examples being welcome.

In addition, respondents considered the Statutory Guidance should clearly set out circumstances in which the ICO will issue an 'urgent' notice. There was also a request for detail about how information obtained via an Information Notice will be handled by the ICO.

One observation made was that the Statutory Guidance doesn't mention that there's nothing in the legislation preventing the ICO from serving an Assessment Notice in case of non-compliance with an Information Notice, as an alternative way of collecting information required on site.

One respondent noted that the text refers to giving an Information Notice to 'an individual' but suggested that this should be to 'a person' since a notice may be given to an organisation, which can be a legal person, and not just to individuals.

Assessment Notices

Respondents requested further details on when an Assessment Notice may be issued, including details about the process and what this entails, along with examples. Some requested information on the risk assessment process used and the methodology for determining the 'likelihood of damage or distress to individuals'. Others wished to know what actions can be included within an Assessment Notice. Furthermore, some felt the Statutory Guidance should set out the factors the ICO will consider when deciding what actions it may take where an organisation fails to respond to an Assessment Notice.

Some respondents expressed clarification on the type of information that may be accessed by the ICO, noting the risks of information relating to fraud or financial crime being compromised. They therefore sought clarification on the issue of the vetting of ICO staff, the role of memoranda of understanding and how the ICO protects sensitive information it may access. It was also noted that although the Statutory Guidance refers to special care being taken when accessing health and social care records, it should recognise that other types of sensitive information can be sensitive and demand similar treatment. Linked to this, it was suggested the Statutory Guidance should specify the basis for processing likely to apply to personal data needed to comply with an Assessment Notice.

Some respondents noted that the text appears to suggest organisations must actively request that access to information as part of an Assessment Notice is limited, whereas the ICO should only be accessing the minimum amount required.

There were several queries about the potential to interview an organisation's staff as part of an Assessment Notice. Respondents indicated they would welcome information about the interview process, who can attend, with some suggesting this should allow, as far as possible, lawyers or union reps. Others queried the issue of obtaining consent for additional interviews, and whether organisations can refuse to make staff available and whether staff themselves can decline to attend. Some felt desk-based interviews were unlikely to be appropriate in

many cases. Other information requested included details about the retention of interview records, and whether the contents of the interview would be made available to the organisation or if they are confidential. It was also suggested the Statutory Guidance should detail whether it may be a criminal offence to provide a false response and what level of responsibility there is within the organisation for any such incidents.

Respondents also requested further details on whether organisations are able to comment on draft audit reports before being published, and to what extent the full report may be published, including whether any identifying information is included in executive summaries.

Another thought that the Statutory Guidance should clarify what category of information request the standard Request For Assessments (RFAs) fall into, as the use of Assessment Notices feels significantly more serious than an RFA. The Statutory Guidance should clarify role of RFAs and how they fit into the scale of enforcement measures.

Enforcement Notices
Respondents requested further information on the types of Enforcement Notices the ICO can issue as. They also requested details of the legal and factual circumstances that would trigger urgent action (eg as a result of an investigation, or in other circumstances). Respondents also requested illustrative examples.

Respondents also wanted more detail about preliminary notices and on making representations. They also wanted to know in what circumstances the ICO may decide not to provide a preliminary Enforcement Notice and to provide any examples.

Some wanted more detail on the relationship of Enforcement Notice and other types of notices, for example, whether an Enforcement Notice would be issued before or after an Assessment Notice. Some felt there was a lack of clarity on the reference to certification/monitoring bodies and their requirements in relation to correcting action.

Some respondents wanted the Statutory Guidance to acknowledge that a stop processing order could shut down some businesses and wanted a commitment from the ICO to first discuss such a notice with the organisation in question. They also wanted the Statutory Guidance to consider the commercial impact of such an order and the feasibility of this. They felt the Statutory Guidance should reflect the ICO's approach of securing voluntary compliance before issuing Enforcement Notices, which could remove the need to take corrective action.

Penalty notices
Several respondents provided a range of comments on the level of detail in the Statutory Guidance on penalty notices.

In terms of notices of intent, a comment received was that the Statutory Guidance doesn't make it clear that this is a legal requirement. Other respondents asked for detail about the process for appealing a notice of intent, and what the ICO would expect to see in any

objection raised. Some wanted clarification whether a penalty notice may be issued before other types of notices.

There were numerous calls for more detail on the way the ICO calculates the amount of a fine (a respondent suggested that the ICO could follow the approach of one of the German supervisory authorities to detailing calculations).

Some raised issues about determining an organisation's turnover, how this is calculated, and the implications for organisations, such as public bodies that don't have turnover. Others wanted further clarity on the time period the turnover is calculated from, given that turnover can change over time, querying if this is the year before the infringement, the year preceding the decision to issue a penalty, or the issuing of the penalty itself. Some also felt that turnover won't be relevant in all cases and doesn't necessarily have a causal link with an infringement, nor is it listed as a factor in either the GDPR or the DPA 2018. Consequently, some felt turnover is not an appropriate measure of culpability and shouldn't be used as a starting point for calculating a penalty amount.

Some felt more clarity is needed for the relative weight attached to each of the factors listed by the ICO that may result in penalty and highlight the extent that certain factors are likely to determine whether to impose penalty or to increase the amount. It was suggested that the Statutory Guidance should clarify what the ICO considers as 'damage', as well as when 'low-level totality of damage' becomes 'substantial'.

Likewise, some respondents wanted clarity on the difference between the standard maximum amount and the higher maximum amount, and examples of when these might apply.

Respondents felt the Statutory Guidance could better explain how culpability and impact on data subjects is determined, as these are not terms used in the GDPR. They also questioned how they will be used when calculating fines. Some felt that the distinction between seriousness and culpability seems arbitrary and that certain factors categorised in the Statutory Guidance as serious have more to do with culpability of an organisation. They felt that using these, along with turnover, risks creating arbitrary and unpredictable starting points for penalties.

Several respondents also commented further on the nine-step process for determining the amount of an administrative penalty. Some respondents felt it represented a good starting point, but that each point may need some further detail and clearer information to be more comprehensive.

Another respondent felt the nine-step process wouldn't result in effective, proportionate, and dissuasive fines. They felt the ICO's approach is at tension with the GDPR and noted the European Data Protection Board's guidelines on issuing fines. For Step 4 of the process, which includes the Penalty starting point table, they questioned what the ICO's legal basis is for such calculations. They also suggested removing this step and also turnover as a factor from Step 1.

Some other comments about the table on page 23 included that it should be made clear why a fine be issued for the lowest starting point if the degree of culpability is low/nil and the seriousness is also low. Another felt the table doesn't appear to reflect the ICO's stated proportionate approach about reserving its powers for the most serious breaches.

One respondent thought the process for calculating penalties doesn't fully reflect the process set out in the GDPR. They considered that any penalty amount should be determined on a case-by-case basis, without any pre-determined figure or percentage. They also considered that the amount should be base solely on the seriousness and nature of the infringement and the organisation's culpability, rather than whether the infringement falls into the higher or lower tier of penalties. They also didn't agree that there should be a reduction for paying the penalty early as part of the calculation of the penalty itself and this should be removed from the guidance. Another was concerned whether the discount for early payment for not appealing a penalty notice impacts on the organisation to a fair and impartial tribunal.

Some wanted further details on how the ICO will calculate a fine when there have been multiple infringements of several articles and how this affects the financial caps that may be applied. Conversely, some felt the Statutory Guidance is less clear about how the ICO will exercise its powers for less serious infringements and what sort of penalty, if at all, might result.

Others wanted to know what is meant by a significant penalty, and linked to this, when is it likely to trigger a panel of non-executive advisers. More details on the panel was requested, as some felt it seemed more of a discretionary rather than a formalised process. They also wanted details of the ability to respond and appeal to the panel.

Some respondents felt the Statutory Guidance should provide a clearer view about how aggravating and mitigating factors are considered, and the extent the starting penalty will be adjusted as a result. They would like to see examples of mitigating and aggravating factors included within the Statutory Guidance. In a similar manner, some respondents felt the Statutory Guidance should emphasise the role of accountability and organisational commitment to compliance, and other behaviours such as mitigating factors the ICO will consider. They felt the Statutory Guidance could actively encourage accountable behaviour by explaining how it will factor accountability into its decisions about regulatory action.

Others also wanted further detail on the ICO's approach to assessing economic impact, the criteria used, as well as how an organisation can challenge the assessment. Some felt the draft Statutory Guidance seems to refer to the impact on the organisation's sector rather than it as an individual business. They wanted to know what alternative there is to fining an organisation if the result could lead to it collapsing. Others wanted the ICO to consider the impact on service users who may be negatively affected by an organisation's funds being diverted to pay for a fine. Still, others thought the assessment of the penalty amount should consider the benefits, including profits, an organisation may have gained from an infringement, noting that for some, their practices are central to business model but may routinely breach data protection law.

Some respondents wanted the Statutory Guidance to clarify the role of other supervisory authorities and what triggers their involvement in the process of determining a fine. They also wanted to know if the organisation subject to the penalty notice will be notified and if they can object to their representations. Respondents also wanted to know how this will apply once the end of transition period from the UK exiting the EU has been completed. Some also wanted to know if they would be fined twice as the UK leaves the one-stop-shop mechanism. Likewise, some wanted to know if the fines will continue to be denominated in Euros.

A respondent noted that there should be stronger or additional sanctions where organisations break their commitment and doesn't find it appropriate that the draft Statutory Guidance removed the intentional character of the failure or the extent of negligence which is listed in the current RAP as a criteria to determine the amount of the penalty.

Another comment was that the draft Statutory Guidance could aid transparency by explaining where the money from a fine goes.

Fixed penalties

Further information respondents would like to see included details of any reminders that may be issued prior to a fixed penalty being applied, and clarification of how the £400, £600 and £4000 amounts have been determined.

One respondent asked for clarity on when a fine is applicable. For example, if an organisation simply forgets to pay the data protection fee, are they given a grace period to resolve this.

Privileged communications

Some respondents queried the definition of what the ICO means by the term 'privileged communications'. Others were unclear why the ICO believes it has powers to review legal privileged communications and asked for clarification of the circumstances the ICO believes it may be able to access such materials. Some suggested that the draft Statutory Guidance proposes a significant change to the ICO's approach on the matter and were concerned why it doesn't explain why this has changed.

Some thought the Statutory Guidance should give an indication of when access to privileged material can be requested by the ICO, and also explain rights of organisations to withhold such information.

Linked to this, some respondents noted that the DPA 2018 requires the ICO to provide guidance on accessing privileged communications, but were concerned the Statutory Guidance merely repeats section 133 and doesn't provided any details on the ways the ICO will assess if communications are privileged or what procedural measures will be used. They considered the current draft Statutory Guidance as insufficient in explaining how the ICO uses its powers in practice to ensure that privileged communications are safeguarded, as required by law. Instead, they were concerned the Statutory Guidance makes unclear statements about the ICO's ability to access such material and simply refers to the Attorney General's guidelines. However, some respondents noted these were produced in 2013, in a different context about criminal investigations and queried how they provide appropriate guidance to

the ICO. Others asked how the ICO will apply the guidelines in practice. Some suggested more detailed and tailored up to date guidance is needed from the ICO on this topic.

Respondents wanted information on the practical steps it will take to protect privileged communications and how it will ensure it only uses it as necessary. Some considered that the Statutory Guidance should confirm that the ICO will itself maintain confidentiality of such communications and reassurance that organisations won't lose privilege in the context of other proceedings due to disclosing the communications to the ICO.

As noted elsewhere, a concern was raised that the Statutory Guidance doesn't appear to cover the law in Scotland, which has a different legal system. The Statutory Guidance should indicate that the ICO will take advice on Scottish law when needed.

Support for controllers and processors

A couple of comments were received that whilst the Statutory Guidance articulates the regulatory measures available to the ICO, it doesn't provide any guidance that supports organisations who may be subject to regulatory action. They felt it would be useful for the Statutory Guidance to set expectations of how the ICO will engage with them. This ties in with other feedback about wanting more detail and clarification of the ICO's approach and how it will use its powers to aid their understanding of how the ICO will take regulatory action.

General feedback

On the consultation process itself, some respondents expressed their view that it was limited to a very narrow range of questions, with a limited range of answers. Given the importance of the Statutory Guidance and its potential to impact on organisations, they felt the consultation process should have been a more detailed and open process, with both a wider and longer response pool.

Another queried whether the consultation process proactively included a diverse and numerous enough range of controllers and processors, noting the wording of section 160(9) of the DPA 2018. It was suggested there should be a more detailed and collaborative consultation with those who will be affected by the Statutory Guidance, including with industry bodies and civil society.

As indicated in other sections of this summary, there were other comments made about a number of issues relating to the Statutory Guidance.

There was particular concern about recognising Scotland's separate legal system applying for criminal prosecutions and legal professional privilege and this was factored into the ICO's regulatory approach.

A query that was raised was how frequently or regularly the Statutory Guidance is going to be reviewed.

Again, there were comments about how other ICO initiatives would be factored into any regulatory action that may be taken, such as an organisation's participation in the ICO Sandbox, or compliance with the ICO Accountability Framework.

As noted under the 'Enforcement' theme, some felt there was a lack of clarity about the ICO's statement about ensuring commercial enterprise not being constrained by regulation, and the implications of this for non-commercial organisations.

There was a suggestion that organisations paying the Data Protection fee should be provided with any reports detailing how the ICO's regulatory action has improved data protection within their sector.

One respondent suggested that input should be received from victims of data breaches and other infringements when issuing penalties.