Call for views on accountability toolkit

Summary of responses and ICO comment

Introduction

On 28 October 2019, the ICO published a survey seeking feedback to inform our views on the development of an accountability toolkit. You can find a copy of the survey here.

The main purpose of the survey was to understand:

- Existing accountability practices;
- What might lead to improvements;
- How the ICO might support organisations in designing their own internal accountability programmes; and
- What scope and structure may be most helpful.

Overall, we received an excellent response to the survey - 163 responses from a variety of stakeholders. The detailed and varied responses provided have given us a much clearer picture of the wide range of tools and resources people are currently using to build effective privacy management programmes.

The positive comments about existing ICO guidance, such as our "Guide to GDPR", will enable us to reflect upon what we are already doing well. Evaluative commentary about where we could improve, including popular features of other resources, will be very valuable as we develop our accountability toolkit itself, and also with respect to our other guidance materials, that will support and complement the toolkit.

The responses have also provided a great deal of insight regarding the practical realities of implementing privacy management programmes. It's helped us to understand more about the main areas of technical challenge and also more general barriers such as commitment to data protection from top management.

It's clear that there is a desire for greater clarity on what 'good looks like' and what an organisation would be expected to do to demonstrate compliance. There were many suggestions about how we could support organisations to improve their accountability, including small to medium enterprises.

Reassuringly, there was a large amount of positive feedback about the idea of a toolkit, as well as the proposed scope and structure, and many helpful comments and suggestions which will assist us to focus on user-needs and possible risks.

We are very grateful to everyone who took the time to respond to this survey. Ultimately, we want to create a product that works for you, and your feedback is fundamental to our considerations. Whilst we cannot reply to each respondent, we have analysed the key themes raised and included our comments.

The next stages of our consultation will involve a London workshop on 3 February 2020. Following further feedback and development, we expect to pilot the toolkit before final publication with practitioners experienced in the day-to-day realities of data protection.

Key themes

Existing practice and guidance

The majority of respondents believed that they had a good understanding of the internal measures that need to be in place to ensure effective data protection compliance, and had general confidence in their organisation.

The Guide to GDPR was the most commonly cited resource that respondents used to develop their understanding of accountability, followed by training and the ICO's self-assessments.

In addition, a wide range of other resources were also cited including primary legislation and guidance from the European Data Protection Board, the IASME Governance Standard, British Standard 10012, ISO27001, OneTrust, the NHS Data Security and Protection (DSP) toolkit, and the Nymity privacy management framework. A couple of respondents had also benefited from an ICO on-site advisory visit.

Respondents also ranked the "Guide to GDPR" as the most helpful of the resources available, explaining that they had most confidence in it as an independent resource from a regulator.

Popular features of the Guide included:

- Easy navigation
- Good balance between technical information and overview that is useful to share
- Plain, user-friendly language
- Bite-sized sections and mini-checklists
- Kept up-to-date and the 'What's new' section.
- Relatable examples based on real world experiences and some templates
- Mapping of requirements to the legislation

Comments about the ICO's self-assessments and checklists (which also form part of the Guide) highlighted the additional benefit of this approach

as a useful way of bench-marking compliance in order to identify weaknesses and providing evidence.

A small number of responses regarding the limitations of our guidance materials tended to focus on the generic nature of the guidance; a lack of sector-specific information, cross-industry examples and the residual need for businesses to incur costs developing their own resources, such as templates, and technical solutions.

Similar reasons tended to be given as to why other resources were being used, for example, training could be more tailored and a consultant could implement practical changes. Many respondents particularly noted the benefits of being able to interact and compare their business practices with others.

The fewest people said they had used a third party privacy management framework. Amongst those that had, respondents again appreciated the potential for more sector-specific frameworks. Aspects respondents liked included a methodology, clear categorisation of activities and descriptions of activities along with example outputs to help communicate the scale of the work to senior management.

Regarding the areas of accountability that respondents found most challenging, contracts and third parties topped the list, followed by records of processing and policies, procedures and training. There were some common themes across all these areas including:

- Organisational complexity and diversity;
- The volume and complexity of information, and keeping it up to date;
- Dealing with others, either internal staff, or third parties who may not have the resources, understanding or who may not be forthcoming with information;
- Uncertainty about how much detail to go into;
- Time consuming nature of tasks and the resource impact; and
- Perception of data protection as not very important, low buy in from senior staff and maintaining staff commitment.

ICO comment:

Respondents expressed general confidence in the measures their organisations had put in place, and the ability to demonstrate compliance. Despite this, the full survey results show that there remains significant room to improve and develop accountability. This is something we've also observed in the audits and investigations we've carried out.

It was great to see how highly regarded the Guide to GDPR is and to hear how much it had supported organisations. Your feedback will help us to develop the toolkit, incorporating positive aspects of the Guide or other resources. It may also help us to develop additional resources to sit alongside the toolkit, such as case studies. We'll also take note of the privacy management challenges highlighted, which are relevant to the toolkit's development as well as our wider suite of guidance.

While we'd anticipate that the toolkit will help to establish universal standards, seeing the toolkit as a complement to the wide range of resources already on offer will clearly continue to be important. While much of our guidance, by its nature, will not be sector-specific, we welcome dialogue with any sectors interested in the opportunity to create sectoral GDPR Article 40 codes of conduct.

Improvements

Respondents described the great deal of effort that had already gone into improving practices following the introduction of the GDPR, and many expressed confidence at having reasonably robust information governance in place.

More generally, many respondents expressed that their organisation always remained open to learning and was dedicated to continuous improvement. It was highlighted that monitoring and review is integral to delivering real and effective data protection, and that is an ongoing process as more guidance and tools become available, good practice is shared, and organisations evolve and grow alongside an ever-changing data environment.

However, the majority of respondents agreed that there was room to improve. Some reflected on the scale of the tasks and the difficulty in 'perfecting' governance, acknowledging that there were some areas that remained weaker than others. Some respondents explained data protection may still be regarded as the sole responsibility of one individual rather than an organisation-wide responsibility. It may be seen as an onerous burden, or a subject that is not very important. Better support from top management for data protection and staff training were seen as key to securing resources, maintaining commitment, and embedding data protection through cultural change.

Demonstrating compliance

Many respondents expressed general confidence in the ability of their organisations to demonstrate compliance with data protection requirements, and reported real investment to get ready for the GDPR.

Respondents referred to regular reviews of compliance, including internal and external audits such as the ICO's advisory visits. Some privacy management frameworks were seen as helpful in this respect, particularly the NHS DSP toolkit.

Despite this, there was clearly scope to improve further. Respondents described uncertainty about drawing the relevant information together to be able to demonstrate compliance if requested, and doing so in a timely manner, noting that information was often 'fragmented' across different departments.

Connected to this issue, some respondents expressed a desire for greater clarity over what the ICO's expectations look like and for easier, more consistent ways of demonstrating compliance. Respondents explained that the uncertainty about this is a challenge, and greater challenges arise when third parties or customers request an organisation to demonstrate their compliance in different ways.

One respondent said that while they were clear about how to demonstrate compliance to a regulator, they were less sure about effective ways to share this message with the public. Another respondent explained that there was still significant trepidation about transparency, stemming from a fear of damaging business brands.

A respondent suggested that the ICO introduce 'spot checks' on accountability to ensure that organisations are properly prepared to demonstrate their compliance.

Information and support

Regarding internal support, there was a mixed response, with some perceiving that their organisation had invested well and recognised the importance of staff awareness and training. Alternatively, while there may be sufficient information available, it was common for respondents to cite a lack of resources and budget dedicated to data protection.

Regarding the level of information and support available externally, generally there was a view that this was sufficient but there was greater concern about the accessibility of information. A common theme was that bigger businesses with access to more resources had a significant advantage because they are able to 'buy in' expertise and materials.

Quite a few considered that helpful resources were too fragmented and you had to 'know where to look', and some also reported that there remained a lot of misinformation.

Generally, respondents thought that there was less information available on the specific subject of demonstrating data protection compliance. Some cited the NHS DSP toolkit as particularly helpful in this area.

Respondents made some suggestions about what additional resources might be helpful including:

- A list of template documentation all in one place to reduce inconsistencies and the cost of buying them from elsewhere;
- More 'end-user' support rather than information targeted at data protection officers with technical expertise;
- More examples on specific and practical scenarios regarding developing an effective privacy management framework within an organisation;
- More clarity on the level of detail required (although it was acknowledged that this depends on the circumstances);
- More videos/webinars from the ICO targeted at different business sectors; and
- ICO to share real life examples of businesses 'doing it right', and encourage greater transparency of business documentation so organisations can see what good accountability looks like

ICO comment:

It's positive that respondents generally expressed confidence in their organisation's accountability and ability to demonstrate this. Respondents also showed encouraging awareness of data protection as an ongoing process of evaluation and improvement.

However, the detailed comments provided also tell us that there remain doubts about the depth of the compliance being achieved and the ability to demonstrate accountability. From the cases we investigate and the audits we carryout, we agree that there is room to improve. And while we appreciate the scale of the task in some cases, organisations cannot be complacent. Accountability is a legal requirement, rather than an optional one.

Respondents indicated that wider cultural change is often still lacking, and said this area offered the most scope for improvement. It's clear from the feedback that respondents would appreciate our help to communicate the value and importance of accountability in order to get

the levels of management 'buy in', training and resources that are required to embed accountability more fully.

It was also clear that the toolkit would be welcomed to help clarify the ICO's expectations, and to help provide a better picture of how to demonstrate compliance in particular, where there was some doubt. Respondents were keen to learn from our extensive supervisory experience and thought this would help support greater consistency, understanding and confidence.

While there's a balance between what we can or should do as a regulator, and what we must expect organisations to take responsibility for, there were many valuable and helpful suggestions made about additional resources that may support the toolkit. There was a strong emphasis on sharing real-life, practical experiences to illustrate how to achieve appropriate accountability and communicate the difference it can make, which we will take on board.

Scope

The majority agreed with the principle that the toolkit should not aim to be exhaustive, recognising the many variations involved and that one size could not fit all. Flexibility in approach was preferred. Many commented that the scope struck them as realistic, reasonable and balanced.

Commonly, respondents thought that it would represent a good 'starting point' and would assist organisations in performing a 'gap analysis'. One comment was that the toolkit seemed like a good complement to existing guidance - a half-way house between reading guidance passively and self-auditing.

Respondents appreciated the toolkit's potential to create more universal standards and a level of consistency, which was broadly welcomed. Respondents also welcomed the toolkit's approach as a helpful way of communicating with management in particular, and supporting engagement.

A note of caution urged was that the scope of the toolkit would need to be particularly well communicated to avoid confusion. While the benefits of toolkits in general were appreciated, some described that they may quickly become 'checklists' and the bar people aim for, rather than the foundations people build upon. The importance of communication with SMEs to avoid over-burdening was also stressed.

Some people made suggestions about how the toolkit could be most effective, including incorporation of practical elements, such as templates and examples to really bring to life what 'good' looks like.

A few expressed doubt over whether the creation of a toolkit should be part of the ICO's role, and queried whether in the example provided in the survey relating to 'management structures' we had been too prescriptive. One comment was that the toolkit should be 'outcome-focused' if it is to be truly scalable. There was some uncertainty about the relationship with other existing frameworks.

A small number of critical responses suggested that the toolkit should aim to be exhaustive, include sector specific or global requirements or that it would have a limited impact on culture if potential fines had not already been enough.

Support for SMEs

Common suggestions for supporting SMEs included checklists, templates, examples, and myth-busting. More targeted step by step guidance, which focused on specific sectors was also suggested.

There was a particular emphasis on templates and model policies that could be easily adapted, including a simple self-audit template. A respondent commented that it was crucial to show this audience not just what we want to see, but also how we want to see it.

Some made suggestions about possible ways to adapt the toolkit to make it more suitable for this audience. A few suggested that it would be particularly helpful to recognise the reality that this group have very limited resources, so resources that support prioritisation were emphasised. Greater clarity on mandatory requirements and how to scale accountability were sought.

A respondent suggested that it would be key to explain the 'spirit of the law' and why certain measures needed to be in place. It was also deemed important to look for ways to challenge the assumption that data protection is too onerous.

ICO comment:

We were reassured by the volume of respondents who agreed with our suggested scope, and who thought we were striking the right balance by not aiming to produce an exhaustive list of requirements.

We note, and agree fully with those who highlighted that it will be particularly important to communicate what the toolkit is and is not intended to achieve, to minimise possible confusion and unintended

consequences (especially regarding SMEs). The relationship of our proposed toolkit to other frameworks, in particular the NHS DSP toolkit, was frequently highlighted and we will consider this carefully.

We are strongly committed to engaging with SMEs. We have recently launched a new SME website hub to make it as easy as possible to find essential guidance, with plans to develop more dedicated resource in 2020. We are grateful for all the ideas to help us develop this area further, and while we anticipate that the toolkit itself would be of most benefit to medium-sized organisations, we will consider whether any adaptations or additional resource may be appropriate.

Proposed toolkit categories

A large majority agreed that the proposed categories for the toolkit were suitable. Respondents generally thought that it represented a good starting point, covering key areas reasonably comprehensively.

Respondents made helpful suggestions about areas that they considered may not fall somewhere under existing headings clearly. Of the areas flagged, the most significant mentions were for risk, records management, and overseas transfers. Drawing helpful comparisons with their organisation's own internal privacy management frameworks, respondents also highlighted areas that were distinctly represented including a clear category about monitoring and engaging with legal developments. One respondent highlighted the importance of training and said this may merit a category in its own right.

There were some suggestions made regarding changes to category names. For example, 'improving' or 'monitoring' were preferred to 'revision'. Some respondents suggested that some of the areas could potentially be merged with others such as the transparency, lawful basis, and DPIAs categories.

Quite a few respondents thought that the order of presentation might be significant and thought that data protection by design and by default and records of processing were fundamentally important to all the other areas. A couple of respondents referred to the 'information lifecycle' approach, and thought that we might try to order our categories in a similar way.

A few respondents raised issues about written style, suggesting that our proposed categories and descriptions could be written in plainer language, particularly for the benefit of smaller organisations.

Expectations and indicators

A large majority favoured our approach to structuring the toolkit in this way. There was a general consensus that this was clear and concise, representing a sensible starting position. Respondents thought this structure finds the right balance, where organisations can decide what's appropriate. It was stressed that it must be clear that neither expectations nor indicators are exhaustive.

Many commented that it was helpful to set out both what is expected and how to measure the effectiveness of systems already in place. Quite a few expressed a preference for a mechanism that allowed a maturity review process. There was a suggestion that a column allowing an organisation to set out 'where the organisation is today' would be helpful for comparison.

There was a perception that the structure might lead to a 'pass or fail' or a 'yes or no' answer, which is too negatively slanted. It was suggested that we encourage a fuller response, with associated evidence or a method for uploading or linking to relevant documents. Some respondents thought that there should be an indication of how to go 'beyond' the indicators of effectiveness.

Some respondents said this approach is broadly aligned with other frameworks of a similar nature such as the NHS DSP toolkit. Respondents thought that this structure was particularly helpful for practitioners who need to design structures and set out what needs to be done for senior management. The structure was deemed to be easily auditable.

Some respondents thought that the structure might be too prescriptive about what organisations should do. One respondent suggested that expectations could instead be represented as 'outcomes' and indicators could then list different means of achieving the desired outcome, with examples drawn from across different practices and organisational sizes.

Following on from the above concern, some thought there was not enough clarity on scalability, particularly for SMEs. Some raised that it would be preferable to be clearer about mandatory requirements, highlighting that many organisations are not required to have a DPO for example.

Respondents emphasised the desirability of plainer language, and punchy bullet points. Some thought the written style was quite wordy and 'audit-based'. There was some concern certain terms might not be readily understood by all or where used imprecisely, such as 'information governance'.

Granularity of detail

The majority said that the level of detail provided in the 'management structure' example in the survey looked about right, achieving a fair balance of information that was not too over-bearing for medium to large organisations.

The most significant concern was about the toolkit's suitability as a resource for smaller organisations, given that it contains details that would not be relevant. Other concerns were that the expectations and indicators could be more clearly defined, and that the differences between them were not always obvious.

Suggestions for improvement more generally included links to the legislation, fuller explanations, templates or examples.

ICO comment:

There was a really encouraging response regarding our proposed categories, with many not only broadly agreeing that we had made a positive start but also saying that it had already begun to influence the thinking and development of internal frameworks. It was great to see the similarly positive reception our approach of 'expectations' and 'indicators of effectiveness' received.

Although we have so far provided a limited example of a work in progress, there were a number of very helpful pointers to help us to consider the overall coverage of the toolkit, how the different categories sit together, and how they are presented.

We are pleased to see that the majority of respondents thought the level of detail being presented was about right. There were a number of fair comments about language and style for us to consider as well. As many acknowledged, other tools we offer are better placed to support smaller organisations in particular. We will continue to consider this dimension and be mindful of the need to place the toolkit in its appropriate context.

Unintended consequences

Respondents expressed that data protection is already seen as an encumbrance to business by some, especially where resources are over-stretched and the toolkit might exacerbate that perception. It was

thought that this would be a particular risk regarding smaller organisations.

Some thought that there may be resistance if the toolkit did not seem to align with current business practices, or where an organisation was already working to comply with another toolkit. This might cause frustration and duplicated effort.

Uncertainty about how to use the toolkit and how to scale it appropriately was also raised. Some respondents thought that the toolkit might be misinterpreted as something that all organisations need to do, leading to substantial costs. Respondents also thought there was a risk the toolkit could be mis-used and taken as 'gospel' by some, resulting in a minimum compliance approach or tick-boxing.

Effective communication was seen as a way to remedy the above, although due to the toolkit's nature, some thought there may be unintended consequences in terms of the effort to correct errors, update the toolkit regularly and the volume of questions that may be posed.

There was concern that the toolkit might be used to represent an organisation's progress too simplistically in terms of a 'pass/fail' and that this might be demotivating for some practitioners who are achieving good outcomes, but not necessarily via the means prescribed in the toolkit.

A few highlighted that the toolkit's impact may be more limited than intended because it does not necessarily resolve more fundamental issues such as culture, resource and training, or may not be enforced sufficiently.

ICO comment:

While we are mindful of the issues raised, earlier responses to the survey offer a counterbalance in the main. It's one of challenges of the toolkit to both provide an appropriate level of direction and also encourage organisations to take responsibility for their own accountability. Responses to the survey indicate we are currently striking a fair balance.

This survey has shown the rich variety of resources organisations are already using to build their accountability, and our intention is for the toolkit not to frustrate that process but act as a complement. It's encouraging that respondents anticipated the toolkit being able to align effectively with existing tools such as the NHS DSP toolkit.

It's been very apparent that user guidance will be crucial to manage expectations about what the toolkit is aiming to do including that it is not exhaustive and will sit appropriately within a suite of other guidance materials. Regarding the toolkit in the longer term, it's a product we are committed to investing in over time, continuing to learn from our own supervisory experiences, its use in practice and keeping it up-to-date as we currently do for our existing "Guide to GDPR".

A common theme across the survey results was to highlight the value and importance of accountability. Protecting personal data has never been more critical as more data is used in increasingly innovative ways. Far from being an encumbrance to businesses, accountability offers a real opportunity to change the cultural fabric of an organisation; minimising the risk of breaches, improving operational efficiency, and building trust and confidence. It's also a legal requirement. We will consider ways we could incorporate this key messaging into the toolkit itself, as well as via supporting resources and communications.

Functions

The most important function respondents wanted from the toolkit was the ability to use the toolkit in stages, followed by:

- ability to download the toolkit and use it offline;
- ability to generate a report
- ability to focus on required elements that are applicable to the business
- ability to rate indicators as incomplete, started or incomplete and;
- ability to suggest further ICO guidance or external information based on responses.

ICO comment:

It's apparent that respondents are keen to see the toolkit develop with features allowing them to measure their effectiveness. Being able to distinguish mandatory legal requirements that all organisations must have in place from other requirements (such as the fact that not all organisations need to have a DPO) was also a common theme throughout the survey.

We are keen that the toolkit is user-focused and meets organisations' needs within the boundaries of our aims. There are clearly many possible options about how the toolkit is presented, how it links to other resources, and how organisations might be able to interactive with it.

The survey responses will help to determine the shape of our toolkit in this first version as well as how it develops over time. This is a topic we expect to be exploring further in our London workshops.