Consultation on GDPR Data Protection Impact Assessment (DPIA) guidance

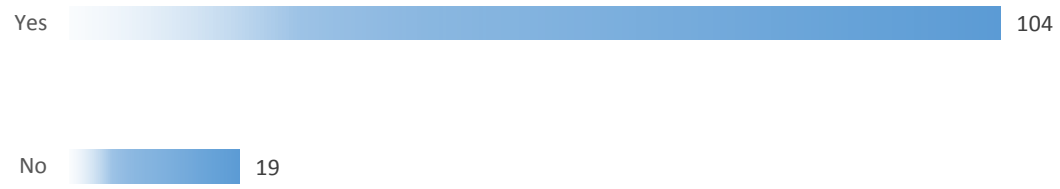
Summary of responses

Introduction

This document summarises the responses to the ICO's consultation on the GDPR DPIA guidance between 22 March and 13 April. There were 126 responses in total and we are grateful to those who took the time to comment. We have carefully considered the views we received and they have assisted us in producing the final version of the code.

Below is a summary of the major themes we have identified in relation to each consultation question.

Question 1 – Is the draft guidance clear and easy to understand?



Responses here generally fell into two camps; those who raised concerns over clarity of the new statutory requirement for their circumstances, and those who commented on the clarity of language and format of the document.

In particular concerns were raised around:

- the length of the guidance and the accessibility of the language used;
- the level of detail of the guidance; and
- the amount of repetition and cross referencing within the document.

ICO Response
As advised in the consultation document, the final guidance will take the form of a series of linked webpages – this will include a contents list on the left hand side of each of the webpages to aid navigation.

Further reading references are included regularly to direct a reader to further detail on specific points. While these are often to the same source document, we anticipate that readers will more frequently navigate directly to pages of interest rather than read the guidance as a whole.

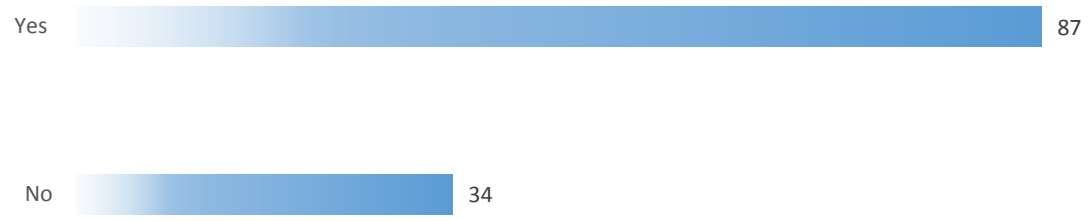
In order to support readers who may navigate to specific sections for reference, key points or principles are repeated, were relevant.

Question 2- Does the guidance contain the right level of detail?

A common request from responders was for examples of high risk, as well as specific risks and possible treatments. There were differing opinions on whether the guidance was too in-depth for small or medium size companies, or too general to be useful to privacy or information security professionals.

ICO Response
We note the concerns of small businesses, and have included specific guidance in DPIAs in our self-assessment toolkits for controllers and processors. https://ico.org.uk/for-organisations/resources-and-support/data-protection-self-assessment/

Question 3 – Does the guidance provide enough clarity on when a DPIA will be required?



Many of these responses referenced the non-exhaustive list of processing activities under Article 35(3), requesting that the guidance provide further detail on GDPR concepts such as 'systematic' and 'large scale'.

Some responses referenced previous PIA guidance, particularly the use of screening questions, as something which organisations were familiar with and had found helpful previously.

Other responses focused on the ICO 35(4) list with specific reference made to new technology, data matching, profiling, denial of service, systematic processing and tracking.

ICO Response

In our Guide to GDPR, we have included a screening checklist of steps a controller should take to assess whether a DPIA is required. This is consistent with other guidance on GDPR responsibilities and has been well received.

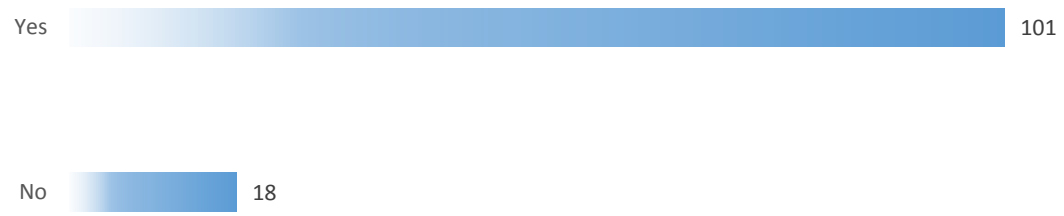
We do suggest that the screening checklist could be adapted locally where a DPIA may be a consideration rather than a requirement. We take on board the responses asking for greater clarity about when a DPIA should be considered.

We note the requests for more practical examples of the processing operations which we consider require a DPIA under the list we are required to publish under Article 35(4). We have now included some illustrative examples of processing operations which we believe would be captured in our list of types of processing that would require a DPIA.

We note requests from another of respondents for more guidance on when a 'small-scale' DPIA would be sufficient. While the terms 'full-scale' and 'small scale' PIA were used in our PIA handbook in 2009, we have referred to PIAs as a scalable process since the publication of our 2014 PIA code. This guidance maintains this position.

DPIAs are designed to be a flexible and scalable tool that you can apply to a wide range of sectors and projects. As our guidance states, conducting a DPIA does not have to be complex or time-consuming in every case, but there must be a level of rigour in proportion to the privacy risks arising.

Question 4 – Does the guidance provide enough clarity on circumstances when you need to contact the ICO?



In general respondents said they were clear on when the requirement to formally contact the ICO, under the Prior Consultation process detailed under Article 36 of GDPR, was engaged.

Some of the comments received suggested some uncertainty remained about whether a DPIA identifying high risk engaged this requirement, or only in circumstances where the controller cannot identify sufficient controls or mitigations to reduce this risk.

Some comments asked if the ICO would compel organisations to resubmit where a completed DPIA was considered to be non-compliant.

ICO Response

Article 35(7) states that a DPIA should, as a minimum, contain:
a) a systematic description of the processing;
b) an assessment of the necessity and proportionality of the processing;
c) an assessment of the risks to rights and freedoms of individuals; and
d) the measures envisaged to address those risks.

The obligation for us to provide formal advice prior to the processing will only be engaged if any assessment includes these considerations, and concludes that the outcome of the assessment is a level of residual high risk which the controller cannot accept. Any response will provide further detail on the reasons why a DPIA has not been considered.

Where we receive a request for formal advice where it is not evident that the above steps have been considered, the DPIA will not be accepted for formal consideration.

In ensuring that they comply with their controller responsibilities regarding DPIAs, a controller may subsequently resubmit a DPIA for formal advice.

Next Steps

We are in the process of considering the comments received in response to the consultation and these will feed into the final web version of the DPIA guidance.

This will include finalising our list of processing activities which will require a DPIA under Article 35(4). This list will be submitted to the European Data Protection Board (EDPB) in May 2018.

For further guidance the GDPR and details of what to expect when can be found on our Data protection reform webpages.