OUR RESPONSE

TO THE INFORMATION COMMISSIONER'S OFFICE CONSULTATION REGARDING DPIA GUIDANCE DATED 22/03/2018

Issue 1: Consultation & Publication of DPIAs

Your consultation paper says:

"[DPIAs] can reassure individuals that you are protecting their interests and have reduced any negative impact on them as much as you can. In some cases the consultation process for a DPIA gives them a chance to have some say in the way their information is used. Conducting and publishing a DPIA can also improve transparency and make it easier for individuals to understand how and why you are using their information" (page 10 of the draft guidance).

Issue 1: Our Response

Regarding the section of guidance identified above, we believe it is unclear for the following two reasons.

Consultation with data subjects:

Article 35(9) GDPR states that "where appropriate, the controller should seek the views of data subjects of data subjects or their representatives on the intended processing". Your guidance mentions the consultation process for a DPIA in line with Article 35(9) but fails to identify when a data controller should consult with its data subjects, how long for and in which circumstances it would be appropriate to do so.

You refer to the controller's ability to not consult where commercially sensitive information is disclosed in the DPIA. It is our view that almost all DPIAs, which are by their nature high risk, are going to certain sensitive commercial information.

Publishing a DPIA:

Your guidance introduces the idea of publishing a DPIA; this is not a requirement under the GDPR. This is not explained nor supported with any examples of when it would be appropriate to publish a DPIA. The ICO has not clarified where the DPIA would be published – would this be directly to the data subjects that may be affected only or on the business' website? It fails to give guidance to businesses about the test between, on the one hand deleting commercially sensitive data and, on the other hand prompting engagement with data subjects and protecting their rights. The guidance should state specifically that it is not a legal obligation to publish.

Our view:

We believe that data controllers would be better supported if the ICO provided clear examples of the types of common scenarios where it would expect data subjects to be consulted and how to make decisions about what to disclose. Without this, businesses may be confused as to when they will be required to consult data subjects which will cause an unnecessary burden on businesses, particularly SMEs or those with limited resource.

We also believe that the ICO should clarify issues regarding publishing a DPIA with clear examples of how and when it would be appropriate to do so. Introducing this additional requirement goes beyond the scope of Article 35(9) and requires justification for doing so.

Issue 2: Prior Consultation with ICO

Your consultation paper says:

"What are the possible outcomes? We will provide you a written response, advising you that:

…

- your DPIA is not compliant and you need to repeat it; or
- the processing would not comply with the GDPR and you should not proceed."

Pages 39 and 40

Issue 2: Our Response

Resubmitting non-compliant DPIAs:

The draft guidance fails to explain whether a DPIA which the ICO has deemed to be non-compliant should be subject to re-submission to the ICO for further review. It must logically be the case that a repeated DPIA which reveals a residual high risk be subject to the duty of consultation, but is the controller's act of failing to complete a compliant DPIA indicative of high risk, and if so, should the ICO specify that this is the case in the earlier sections of the draft guidance regarding risk? Put simply, will the ICO compel controllers to resubmit non-compliant DPIAs to ensure that the controller has learned how to properly investigate and record risk in the DPIA process?

Ban on processing:

The draft guidance fails to provide any examples of when the ICO may expect to compel a controller not to proceed with processing activities. Whilst we recognise that the GDPR creates such rights for the ICO we know that many businesses that we represent would find the idea of any national supervisory authority interfering with their commercial activities before they have been commissioned to be abhorrent. The draft guidance fails to say whether such a decision from the ICO would be rare or how it would monitor any such ban.

The relevant Article of the GDPR describes the ICO's corrective power as follows: "to impose a temporary or definitive limitation including a ban on processing." The draft guidance fails to provide guidance on the temporary or definite. We believe this would be of value to UK businesses and those advising them.

Our view:

Our view is that the draft guidance should provide very clear parameters about the ICO's actions when a DPIA requires resubmission and the guidance should be updated to reflect this. The references to a ban on processing are very unhelpful because they fail to provide any meaningful detail about this draconian measure and do not expound the nuances of the language in the GDPR, which would be of great assistance to UK businesses and those advising them.

Issue 3: High Risk

Your consultation paper aims to explain what key phrases such as "high risk", "likely to result in high risk", "new technologies" and "large scale" mean.

Issue 3: Our Response

Lack of Examples:

There is a concerning absence of hypothetical of examples relating to what kinds of processing constitute high risk. Whilst we are given some direction as to what constitutes "large scale" and "new technologies", we are left asking about the other examples given by the ICO. To what extent does processing of "biometrics" or "data matching" prompt a DPIA? In respect of "data matching", surely it is not on every occasion that when personal data is combined or matched between departments in an organisation that a DPIA is required? Surely that requires something that goes over and above what the GDPR requires? Furthermore, does profiling children include the day-to-day record-keeping carried out by schools? Does the mere fact that schools keep pupil data mean that a DPIA is necessary? Some clarity here would be greatly appreciated.

On a general point, we have worked closely with representatives in the education sector and the general consensus is that the education sector seems to receive little attention or provide influence in regulatory guidance. We ask, on behalf of the education sector, that appropriate support is given to schools and universities within written guidance in general.

Our View:

Our view is that it is possible and achievable to give examples of high risk processing which can be applied across a number of sectors. Organisations across the country would benefit significantly if they were guided with examples and the DPIA seems like the most obvious area of the GDPR where plentiful examples would make sense. Instead, we are left with more questions that answers.

Issue 4: Lack of Hypothetical Examples

Your guidance fails to provide any hypothetical examples. This omission is a significant failing in the document. Of all of the guidance produced by the ICO, we consider that this guidance is the one which would benefit the most from a reasonable volume of mock examples which businesses can rely on to help make judgements about all of the key issues raised by DPIAs.

Issue 4: Our Response

You should develop a series of hypothetical examples for each of the key areas of your guidance.

Issue 5: New Technologies

Your consultation paper says:

"Using technologies to process personal data in novel or unexpected ways is likely to be inherently more risky than using technologies that are tried and tested, as the practical implications will not yet be fully understood".

And

"If you are planning to use technology you have not used before, even if it is not brand new, we recommend that you still do a DPIA".

(page 20 of the draft guidance)

Issue 5: Our Response

Practical Issues:

These statements appear contradictory.

The latter sentence would suggest that old technologies, already used and implemented by businesses, may also require a DPIA.

What is the position if a DPIA on existing "old" technologies identifies a high level of risk, that cannot be reduced? Under the guidance, this would give rise to the need to consult the ICO, with a maximum of 14 weeks, where an outcome could be to stop using the technology altogether. This could result is high commercial costs and risks to businesses.

Our view:

We ask the ICO to include provisions in the guidance which explain to businesses the extent to which they will need to review old technologies.

Issue 6: Impact on society

Your consultation paper says:

"The focus is on the potential for harm –- to individuals or to society at large, whether it is physical, material or nonmaterial." - page 8 of the draft guidance (our emphasis added).

"The impact on society as a whole may also be a relevant risk factor. For example, it may be a significant risk if your intended processing leads to a loss of public trust." - page 12 of the draft guidance (our emphasis added).

Issue 6: Our Response

Regarding the sections of guidance identified above, we believe that this is unclear, unquantifiable, and unnecessarily increases the risk of non-compliance for businesses.

Both Article 35(1) and Recital 75 of the GDPR refer to data subjects that the processing may impact upon; no reference is made to "society as a whole". All previous guidance materials issued by the ICO focus on the potential harm on the rights and freedoms of the individual data subject when processing personal data rather than the society at large. We believe that this section of guidance goes beyond the scope of what is required under the GDPR and places an unnecessary burden on businesses.

We ask the ICO to consider how it could provide better guidance about how businesses of all sizes are expected to measure what constitutes a risk to society at large. Issues presented by our clients, contacts and other privacy professionals include things such as:

- What constitutes "society at large"? Does this mean that data subjects and society at large need to be separately addressed and assessed?
- What happens if there are conflicts between the impact on the data subjects and the "society"?
- What constitutes a risk to "society at large" or an "impact on society as a whole"?
- What practical examples can the ICO provide what would constitute a high risk to society at large?

Our View:

Our view is that establishing an impact on "society as a whole" or "society at large" is too intangible and subjective to be able to be assessed objectively. We believe that the ICO should reconsider this criterion; alternatively it would benefit from further elaboration and some examples as to what would constitute an impact on society as a whole.

Get in touch

If you would like to speak us further about our response, please contact Matthew whose details are listed below.

MATTHEW HOLMAN
PRINCIPAL

0345 074 2433
matthew.holman@emwllp.com