Centre for Information Policy Leadership
Hunton Andrews Kurth

12 April 2018

CENTRE FOR INFORMATION POLICY LEADERSHIP RESPONSE
UK ICO CONSULTATION ON GDPR DPIA GUIDANCE

The Centre for Information Policy Leadership at Hunton Andrews Kurth LLP (CIPL)[1] welcomes this opportunity to respond to the UK Information Commissioner's Office (ICO) on its draft guidelines on Data Protection Impact Assessments (Draft Guidelines). The Draft Guidelines provide a useful overview of the DPIA process generally, and will be useful for organisations of all sizes, especially for SMEs. CIPL also welcomes the ICO's provision of a non-mandatory sample DPIA template which can provide less mature and especially SME organisations with a starting point in carrying out their own impact assessments.

As an overarching, general comment, CIPL recommends the ICO ensures that the guidelines align as much as possible with the guidelines of the Article 29 Working Party[2] (WP29) to ensure consistency in interpreting the GDPR DPIA requirements and to minimise divergence in line with the harmonisation goals of the GDPR. Organisations operating across the EU need to adopt a single DPIA methodology (including the criteria for triggering a DPIA or assessment of a high risk) and a single DPIA process to deploy for their numerous data processing activities – any divergences in practices by DPAs on this particular point would make this impossible.

CIPL has the following specific comments on the document:

Comments

1. **When to Carry Out a DPIA?** (pages 14 and 16): The Draft Guidelines state that where there is no specific indication of likely high risk, it is good practice to carry out a DPIA for major new projects using personal data and also recommend that if there is any doubt as to whether a processing is likely to result in high risk, a DPIA should be carried out nonetheless. This approach goes beyond the scope of the requirements of the GDPR and also skips a valuable first step of an initial or preliminary risk assessment to determine whether there is a likely high risk. Organisations must be permitted to engage in an initial pre-screening of their processing activities and should only be required to carry

[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 60 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] Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purpose of Regulation 2016/679, adopted on 4 April 2017 And last Revised and Adopted on 4 October 2017, 17 /EN WP 248 rev. 01, at http://ec.europa.eu/newsroom/document.cfm?doc_id=47711.

out a full-blown formal DPIA in cases where the screening or preliminary risk assessment indicates the processing is likely to result in a high risk. Imposing a requirement to carry out DPIAs when there is any instance of doubt or when engaging in new processing is not something that businesses can effectively operationalise. Indeed, the ICO itself refers to such a high level screening test on page 16 of the Draft Guidelines. CIPL recommends that the ICO emphasise and strengthen this point in relation to processing where it is not clear whether a DPIA is required or where an organisation is engaging in new major projects. This ensures DPIAs are reserved for processing operations that are likely to result in a high risk (based on severity and likelihood) and do not lead to a plethora of downgraded risk assessments by companies who will be overburdened by having to carry out full DPIAs for the majority of their processing operations.[3]

2. **ICO List of Processing Operations Subject to a DPIA** (pages 14 and 17): In accordance with Article 35(4), the ICO has put forward a list of additional circumstances which require a DPIA. CIPL would like to express our concern that individual DPAs are issuing their own lists of high risks factors that differ from each other and from country to country across the EU. This makes it difficult for organisations operating across the EU to implement and operationalize an efficient and coherent DPIA process within their organisations. Thus, we recommend that all efforts be made to ensure consistency between the ICO guidance on this issue and the guidance of the WP29.

   Moreover, CIPL recommends the ICO make clear that the processing operations in the list do not mandate a DPIA unless a pre-screen or preliminary risk assessment by the organisation demonstrates that the processing operation is likely to result in a high risk to the rights and freedoms of individuals pursuant to Article 35(1). The flexibility to allow organisations to pre-screen such processing activities is vital to ensure organisations are not unduly burdened both in terms of resources and administrative efforts in carrying out DPIAs on processing that is not likely to result in a high risk. Controllers will, of course, still have to be able to explain and justify their conclusion, based on such pre-screening or preliminary risk assessments, that there is not a likelihood of high risk with regard to the specific processing.

   For example, the ICO ancillary list on page 14 contains "use of new technologies" (See also, "New technologies . . . (including AI)" on page 17) as one scenario requiring a DPIA. CIPL suggests that the ICO highlight that it is not the mere use of new technology (including AI) alone that renders an automatic need for a DPIA but rather whether it is likely the new technology will result in a high risk to the rights and freedoms of individuals. In other words, the new technology must be accompanied by specific or

[3] See also Comments by the Centre for Information Policy Leadership on the Article 29 Data Protection Working Party's "Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is 'likely to result in a high risk' for the purposes of Regulation 2016/679", 19 May 2017, at page 3, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_comments_on_the_wp29s_guidelines_on_dpias_and_likely_high_risk_19_may_2017-c.pdf.

additional risk elements that warrant a DPIA. As noted in CIPL's previous papers on risk,[4] "using new technology" should not be deemed a *per se* trigger for high risk status or a DPIA, but must be coupled with additional high risk characteristics, based on context, scope and purpose of processing. Indeed, the WP29, in its guidelines on DPIAs,[5] notes that while in some cases one high risk criterion may be sufficient, "in most cases" more is needed, i.e., in most cases a controller can consider that a processing meeting two criteria [in the WP29 ancillary list of circumstances requiring a DPIA] would require a DPIA to be carried out. But even a "two criteria" trigger may not be the best approach. CIPL believes that rather than focusing on the number of criteria, the better approach would be to simply allow for and expect an initial, preliminary risk assessment based on relevant factors to determine whether there is a likely high risk that would warrant a DPIA. Thus, organisations will have to make a context specific determination and screen new technologies to understand whether they likely result in such high risk and if the results of the screen do not indicate this, then a DPIA should not be mandatory solely by virtue of the fact that the technology is new.

Moreover, the ICO list of triggers for a DPIA includes large scale profiling and data matching. Profiling and matching data are key computing functions in the modern digital economy and should not trigger a DPIA *per se*. For instance, there may be all kinds of trivial matching of different datasets that would not likely result in a high risk for individuals. In certain circumstances, profiling and data matching are actually essential to protect individuals. For example:

- In the banking sector, profiling and data matching are used for fraud monitoring and to prevent identity theft. They also enable regulated entities to adhere to financial regulations that require end-user authentication to ensure the payment networks that individuals use every data are secure.

- In the information security context, profiling and data matching are used for the automated screening of security flaws and security risk identification, the detection and prevention of cyber incidents, as well as, network and information protection generally.

The key point the ICO should emphasise is that it is not simply the existence of new technologies, profiling or data matching or other factors alone that will trigger an automatic need to carry out a DPIA but whether these activities combined with

[4] See CIPL white paper "Risk, High Risk, Risk Assessments and Data Protection Impact Assessments under the GDPR", 21 December 2016, at page 30, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_gdpr_project_risk_white_paper_21_december_2016.pdf and Comments by the Centre for Information Policy Leadership on the Article 29 Data Protection Working Party's "Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is 'likely to result in a high risk' for the purposes of Regulation 2016/679", 19 May 2017, footnote 3 above, at page 3.

[5] See footnote 2.

additional high risk characteristics, based on the context, scope and purpose of processing are likely to result in a high risk to the rights and freedoms of individuals.

3. **Denial of Service** (pages 17 and 41): According to the Draft Guidelines, using profiling, automated decision-making (ADM) or special category data to help decide on access to services, opportunities or benefits would require a DPIA. CIPL believes that the ICO should clarify this elaboration to provide more certainty on the scope of denial of services by specifying a DPIA is required in this case only where the result of the decision to deny access to services results in a legal or similarly significant effect on the individual. Additionally, the Draft Guidelines should align with the WP29's final guidelines on Profiling and Automated Decision-making in which the WP29 cited examples that indicate a narrow scope of what it means to deny access to a service, entitlement or benefit to something that has a true legal or similarly significant effect on a person.[6] For example, the denial of a social benefit granted by law or the denial of access to an employment opportunity, education or credit. CIPL suggests the ICO add the following language on page 41: "Use profiling, automated decision-making or special category data to help make decisions on someone's access to a service, opportunity or benefit <u>in ways that would have a legal effect or otherwise similarly significant affect that person</u>."

   Note also that on page 17, a section heading refers to "Systematic and extensive profiling with significant effects." We suggest changing this to "Systematic and extensive automated decision-making with significant effects," as profiling is just a step towards ADM and profiling *per se* is not an example of default high risk processing unless it is part of an automated decision that produces legal or similarly significant effects. It is important to be precise about the use of this particular terminology to avoid exacerbating the existing confusion among organisations around the concept of profiling as opposed to ADM in the GDPR.

4. **Meaning of "Significantly Affects"** (page 21): The ICO notes that a significant effect is "something that has a noticeable impact on an individual and can affect their circumstances, behaviour or choices in a significant way". The guidance continues to note that "[a] similarly significant effect might include something that affects a person's financial status, health, reputation, access to services or other economic or social opportunities. Decisions that have little impact generally could still have a significant effect on more vulnerable people, such as children." While CIPL agrees that the ICO's description of a similarly significant effect is accurate depending on the specific context involved, CIPL suggests the ICO highlight that a similarly significant effect is one that rises to a similar level of impact as a legal effect and this is a very high bar to reach. There could be impacts on a person's behaviour or choices resulting from an automated decision that do not reach the level of being similarly significant to a legal effect and the

[6] Guidelines on Automated Individual Decision-making and Profiling for the Purposes of Regulation 2016/679, adopted on 3 October 2017 and Last Revised and Adopted on 6 February 2018, available at http://ec.europa.eu/newsroom/article29/document.cfm?doc_id=49826 at pages 21-22.

guidance should make this clear. Thus, the ICO should confirm that a DPIA is mandatory only where solely automated decisions are made that produce legal effects or similarly significant effects and this is a high threshold to meet.

5. **Seeking Input from Individuals** (pages 6, 25, 30 and 31): The Draft Guidelines state that controllers "should" consult with individuals or their representatives whose personal data may be processed wherever possible unless there is a good reason not to, and where they choose not to do so, they should record the decision as part of the DPIA.

   Firstly, for most organisations, in both the private and public sectors, it would be impracticable, impossible and commercially unviable to consult with individuals on every DPIA. The DPIA must be carried out for many processing operations and the Draft Guidelines already recommend that DPIAs be carried out as a best practice even if it is not clear whether the processing requires a DPIA or if the organisation is engaged in a new major project that involves the processing of personal data (See CIPL's recommendation with respect to this point in Section 1 above). For large and complex organisations, such an approach could potentially result in hundreds of DPIAs per organisation per year at a minimum. Organisations will be completely overburdened if individuals have to be consulted within each DPIA process.

   Secondly, the text of the GDPR requires that the views of individuals be sought "where appropriate" and not whenever possible. Circumstances may exist which may render consultation with individuals inappropriate. The GDPR notes that the controller should seek the views of individuals without prejudice to the protection of commercial or public interests or the security of processing operations. Indeed, there may be valid reasons to not seek such input especially if the security of processing, company IP or commercial or public interests will be severely compromised as a result.

   Thirdly, one must remember that where controllers are unable to seek the views of individuals, controllers can still seek and receive useful feedback about the effectiveness of their transparency, and the potential privacy impact of their data processing through other methods, including through formal and informal interactions and conversations with industry groups, consumer advocacy groups and regulatory bodies.[7]

   Fourthly, with respect to the "how do we carry out a DPIA" wheel on page 25, CIPL believes that the order of point 3 "consider consultation" is incorrect. We recommend that any consultation with individuals or their representatives (where appropriate) should come after the risk assessment has been completed and the mitigations decided, i.e., after point 6 "identify measures to mitigate risk".

[7] See also discussion of "seeking views of data subjects" in the Comments by the Centre for Information Policy Leadership on the Article 29 Data Protection Working Party's "Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is 'likely to result in a high risk' for the purposes of Regulation 2016/679", 19 May 2017, footnote 3 above, at pages 10-11.

6. **How Do We Carry Out a DPIA?** (pages 25 and 32): The Draft Guidelines include assessing necessity and proportionality as one of the key steps in the DPIA process. The ICO describes this assessment as including a full compliance assessment of how a project will comply with all the requirements of the GDPR (e.g. including relevant details of your lawful basis of processing, how you intend to ensure data security and data minimisation, how you support individual rights and safeguards for transfers, etc.) (See page 32 for the full description). CIPL believes that assessing necessity and proportionality is a more narrow analysis (i.e. a purpose-risk-benefit analysis) than a full compliance assessment and the ICO should reflect this in the assessment description. CIPL further recommends the ICO add a separate point to the DPIA process labelled "GDPR requirements and compliance assessment" to encompass the other GDPR requirements. Conducting a GDPR compliance assessment is a fundamental part of the DPIA process and is linked to mitigations as through compliance, risks are mitigated. CIPL suggests the ICO separate out these two points and make it clear that they involve separate activities but both are necessary for carrying out a DPIA.

7. **ICO Risk Management Support** (page 11): The Draft Guidelines recommend that DPIAs should be reviewed when external changes to the wider context of the processing occur, for example, if a new public concern is raised over the processing. CIPL recommends that the Draft Guidelines highlight the role the ICO will play to inform organisations about such "public concerns" (e.g. as demonstrated by a number of complaints or requests for information to the ICO) or other external events that could trigger such DPIA reviews.

8. **Benefits of Processing** (pages 30 and 35): The Draft Guidelines correctly point out that considering the expected benefits of the processing for the organisation or society as a whole is an appropriate consideration in the DPIA process (See page 30). The Draft Guidelines further clarify that in carrying out a DPIA organisations do not always have to eliminate every risk but may decide that some risks, and even a high risk, are acceptable given the benefits of the processing and the difficulties of the mitigation. However, if there is still a high risk, organisations need to consult the ICO before they can go ahead with the processing (See page 35).

   CIPL recommends three clarifications with respect to the concept of benefits:

   a. Add the role of benefits to the "at a glance" section on page 2 of the Draft Guidelines. Currently, there is no mention of the important role of benefits in the summary of the Draft Guidelines. CIPL proposes the bullet could state: "If you identify a high risk that cannot be effectively mitigated without unreasonably impairing the desired benefits of the processing, it may be possible to proceed with the processing but you must consult the ICO first."

   b. In the discussion on the purpose (and benefit) of processing on page 30 and on "necessity and proportionality" on page 32, the guidelines might clarify that the proportionality calculation between the risks of the processing and the benefits

may vary depending on their respective significance. Thus, in a case in which the desired benefits are significant, the proportionality calculation with regard to the risk may be different compared to cases in which the benefits are less significant. In other words, the ultimate assessment of the degree of risk is relative to the ultimate assessment of benefits.

c. CIPL recommends that the Draft Guidelines should highlight the importance of "reticence risk" to the DPIA process. CIPL believes an impact assessment should also consider the failure to pursue certain purposes, interests and benefits of processing in terms of the risk and potential harms that would follow from not pursuing them. This is known as reticence risk or the risk of not engaging in processing that would bring about benefits to various stakeholders and society. Instead of asking "what will we (or third parties) gain from this processing activity?" organisations would ask "what will we (or third parties) lose if we do not pursue this processing activity or if we were to pursue it in a diminished fashion?" This consideration measures the cost of inaction, which is not merely the intended benefit. We believe that this issue could be part of the consultations between organisations and the ICO in connection with a DPIA that identified a high risk that cannot be effectively mitigated without unreasonably diminishing the benefits. In such a case, part of the analysis by the ICO and the organisation could be what are the costs of not pursuing this processing activity?

Conclusion

We hope the above recommendations provide useful input into finalising the ICO consultation on DPIAs. CIPL appreciates the ICO's work in this area, the constructive and outcome based nature of the guidelines and the transparent way the ICO is seeking input. We look forward to continued dialogue between the ICO and organisations on these issues.

If you would like to discuss any of these issues further or require additional information, please contact Bojana Bellamy, bbellamy@huntonak.com, Markus Heyder, mheyder@huntonak.com or Sam Grogan, sgrogan@huntonak.com.