Centre for Information Policy Leadership
Hunton Andrews Kurth

4 July 2018

CENTRE FOR INFORMATION POLICY LEADERSHIP RESPONSE
IRISH DATA PROTECTION COMMISSION CONSULTATION ON DRAFT LIST OF TYPES OF DATA PROCESSING OPERATIONS WHICH REQUIRE A DATA PROTECTION IMPACT ASSESSMENT

The Centre for Information Policy Leadership at Hunton Andrews Kurth LLP (CIPL)[1] welcomes this opportunity to respond to the Irish Data Protection Commission (DPC) consultation on its draft list of types of data processing operations which require a data protection impact assessment (Draft Guidelines). The Draft Guidelines provide a useful overview of the requirements for a DPIA, and will be useful for organisations of all sizes, especially for SMEs.

As an overarching, general comment, CIPL recommends the DPC 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.

CIPL has the following specific comments on the document:

Comments

1. **DPC list of types of data processing requiring a DPIA** (pages 2 and 3): In accordance with Article 35(4), the DPC has put forward a list of additional circumstances which require a DPIA. CIPL would like to express its 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 operationalise an efficient and coherent DPIA process within their organisations. Thus, we recommend that all efforts be made to ensure consistency between the DPC guidance on this issue and the guidance of the WP29.

   In addition, the Draft Guidelines specify that the DPC is proposing a DPIA is required where an organisation engages in the one of the eleven different types of processing

[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. Please note that this document refers to the WP29 guidelines but the current EDPB endorsed these guidelines on 25 May 2018 https://edpb.europa.eu/sites/edpb/files/files/news/endorsement_of_wp29_documents_en_0.pdf.

operations in the DPC's ancillary list (emphasis added). CIPL recommends the DPC 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 DPC's list includes "profiling individuals on a large scale" and "combine, link or cross-reference separate datasets where such linking contributes to profiling or behavioural analysis of individuals." Profiling and cross referencing datasets 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 cross-referencing of different datasets that would not likely result in a high risk for individuals. In certain circumstances, profiling and cross-referencing are actually essential to protect individuals. For example:

- In the banking sector, profiling and cross-referencing 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 day are secure.

- In the information security context, profiling and cross-referencing 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 DPC should emphasise is that it is not simply the existence of profiling or cross-referencing of data sets alone that will trigger an automatic need to carry out a DPIA but whether these activities combined with 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. The same is true for all eleven types of processing contained in the DPC's ancillary list.

2. **Denial of service** (page 3): The DPC also includes in its ancillary list of processing operations requiring a DPIA the use of "profiling or special category data to determine access to services". CIPL believes that the DPC should clarify this by specifying a DPIA is required in this case only where the result of a 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 where 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.[3] 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 DPC add the following language: "Use profiling or special category data to determine access to services in ways that would have a legal effect or otherwise similarly significantly affect that person."

3. **Carrying out a DPIA where there is no indication of likely high risk** (page 3): After the DPC list of ancillary processing operations requiring a DPIA, the Draft Guidelines note that "it is good practice to carry out a DPIA for any major new project involving the use of personal data, even if there is no specific indication of likely high risk". 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 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. The DPC refers to such high level screening on page 5 of the Draft Guidelines where it notes "[d]uring screening there are certain factors that can be considered at a high level to help guide whether a DPIA should be conducted in order to work out in detail whether a high risk exists". CIPL recommends the DPC 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.[4]

4. **What does "significantly affect" mean?** (page 4): The DPC correctly notes that the term "significantly affect" is not defined in the GDPR but that it is used alongside the term "legal effect". The Draft Guidelines continue by noting that "[b]oth are outcomes that have a detrimental or discriminatory effect on an individual or that cause a change in behaviour, decision making, circumstances or the ability to avail of their rights or entitlements. The significance of processing is closely related to the vulnerability of the data subject affected." While CIPL agrees that the DPC's description of a similarly

[3] 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.

[4] 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.

significant effect is accurate depending on the specific context involved, CIPL suggests the DPC further emphasise 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. For example, there could be impacts on a person's behaviour or decision making resulting from an automated decision that do not reach the level of being similarly significant to a legal effect and the guidance should make this clear. Thus, the DPC should confirm that a DPIA is mandatory only where there is a systematic and extensive evaluation of personal aspects of an individual which is based on automated processing, including profiling, and on which a decision is made that produces legal effects or similarly significant effects and that this is a high threshold to meet.

5. **What factors can lead to "high risk" processing** (page 5): The Draft Guidelines include a list of factors which a data controller may considered in determining if a particular processing operation is likely to result in a high risk which in turn warrants carrying out a DPIA. It appears that among the ten factors listed by the DPC, eight of them are already included in the WP29 guidance on DPIA and high risk,[5] while two of them are new (ex-EEA data transfers depending on the envisaged country of destination and the possibility of further onward transfers and insufficient protection against unauthorized reversal of pseudonymisation). Again CIPL would like to express its concern that issuing lists of high risks factors that differ from WP29 factors and from country to country across the EU makes it extremely challenging for organisations operating across several EU countries to implement and operationalise an efficient and coherent DPIA process within their organisations. Thus, we recommend that all efforts be made to ensure consistency between the DPC guidance and the guidance of the WP29.

   With respect to "[u]ses of new or novel technologies", CIPL takes the view that 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. CIPL recommends that the Irish DPC emphasise in the final guidelines that it is not simply the existence of new technologies alone that will result in high risk processing but rather uses of new technologies accompanied by specific additional risk elements.

   In addition, inclusion of the factor of "ex-EEA data transfers depending on the envisaged country of destination and the possibility of further onward transfers" in the list of factors that can lead to high risk processing should be reconsidered. In respect of risks associated with data transferred across borders, Recital 116 of the GDPR only refers to "increased risk", which is different from "high risk". Moreover, any "increased risk" associated with transferring data across borders should according to this Recital, be mitigated by the DPAs and the Commission through relevant cooperation structures with their foreign counterparts. In addition, under the GDPR, as long as the provisions of Chapter 5 are complied with by organisations, transfers outside the EEA should be possible without also requiring DPIAs based on the mere fact of transfer. Article 44 is

[5] Supra note 2 at page 9.

clear in this respect when it provides that "all provisions in this chapter shall be applied in order to ensure that the level of protection of natural persons guaranteed by this regulation is not undermined". Thus, compliance with all applicable Chapter 5 transfer requirements should eliminate any concerns that the transfers at issue themselves impose "high risks". In addition, none of the articles of Chapter 5 mention the need to perform any DPIA or the notion of high risk. Finally, as already stated above, this risk factor is not included in the list of factors published by the WP29.

6. **Number of factors** (page 5): The Draft Guidelines note that "where these factors [that can lead to "high risk" processing] are involved in the proposed processing operation, there is a chance they are likely to result in a high risk, particularly where more than one is a factor" (emphasis added). This line of thought follows the WP29 which mentioned in its final guidelines on DPIA that "in most cases, a data controller can consider that a processing meeting two criteria [from the WP29 list of factors] would require a DPIA to be carried out…[h]owever, in some cases, a data controller can consider that a processing meeting only one of these criteria requires a DPIA".[6] 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 if the results of their screening do not indicate a likely high risk then a DPIA should not be mandatory solely by virtue of the fact that the processing operation involves some of the factors contained in the DPC's list.

Conclusion

We hope the above recommendations provide useful input into finalising the Irish DPC's guidelines on DPIA. CIPL appreciates the DPC's work in this area, the constructive and outcome based nature of the guidelines and the transparent way the DPC is seeking input. We look forward to continued dialogue between the DPC 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, Nathalie Laneret, nlaneret@huntonAK.com, or Sam Grogan, sgrogan@huntonAK.com.

[6] Supra note 2 at page 11.