Centre for Information Policy Leadership
Hunton Andrews Kurth

9 August 2018

CENTRE FOR INFORMATION POLICY LEADERSHIP COMMENTS ON DATA PROTECTION AUTHORITIES' DRAFT LIST OF TYPES OF DATA PROCESSING OPERATIONS WHICH REQUIRE OR DO NOT REQUIRE A DATA PROTECTION IMPACT ASSESSMENT

Under Articles 35(4) and 35(5) of the GDPR, Data Protection Authorities (DPAs) are currently establishing national lists of processing operations that are subject or not subject to the requirement of carrying out a Data Protection Impact Assessment (DPIA) and are communicating these lists to the European Data Protection Board (EDPB). As per Articles 35(6),[1] 63 and 64[2] of the GDPR, the EDPB shall issue an opinion in line with the consistency mechanism.

The Centre for Information Policy Leadership at Hunton Andrews Kurth LLP (CIPL)[3] welcomes the opportunity to provide comments on lists that several DPAs have issued on data processing operations for which a DPIA is mandatory as per Article 35(4) of the GDPR ("black lists") or operations for which a DPIA is not required as per Article 35(5) of the GDPR ("white lists")[4] and how the consistency mechanism should apply in these instances.

These additional comments[5] follow CIPL's previous White Paper on Risk, High Risk, Risk Assessment and Data Protection Impact Assessments under the GDPR,[6] its comments on the Article 29 Data Protection Working Party's (WP29) "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" adopted on 4 April 2017[7] and CIPL's more recent comments made in the context of the UK ICO consultation on GDPR DPIA guidance[8] and the Irish Data Protection Commission consultation on a draft list of types of data processing operations which require a data protection impact assessment.[9] The latter two responses are attached in Annex 2 of this document.

As a preliminary comment, CIPL wishes to reinforce what it already emphasised in these previous papers. These papers argued that the following principles should govern the establishment of any criteria designed to serve as reference for risk assessment and in particular for the identification of whether a processing is likely to result in a high risk for the purpose of the GDPR:

- DPIAs, risk assessments and the notion of high risk are context-specific and organisations must have flexibility to devise risk assessment frameworks and methodologies that are appropriate to the context of a particular processing activity;

- Guidance should include criteria and factors for identifying high risk as opposed to a fixed list of *per* se high risk processing activities that may include processing that might not be high risk in some contexts and that would quickly become outdated because of changed circumstances and rapid technological developments;

- It should be possible for organisations to use a single DPIA to assess multiple processing operations that present reasonably similar risks in order to avoid duplicative risk assessment for similar processing as long as these organisations are able to explain the rationale for their interpretation and action;

- DPAs' lists must align as much as possible with the WP29/EDPB Guidelines on DPIA[10] to ensure clarity and consistency in interpreting the GDPR DPIA requirements and to minimise divergence in line with the harmonisation goals of the GDPR; and

- "Prior consultation" with DPAs under Article 36 of the GDPR should remain exceptional and left for cases where the residual risk is high and the data controller acknowledges that it cannot be mitigated.

Discussion

As mentioned in the Guidelines,[11] "DPIA is a process for building and demonstrating compliance"; DPIAs "are a useful way for data controllers to implement data processing systems that comply with the GDPR" and a "key part of complying with the Regulation when high risk data processing is planned or is taking place". In support of the EDPB's goal of advancing a common understanding of which processing operations require a DPIA, it is important that the criteria remain clear, consistent, pragmatic and easy to understand. Criteria should be consistent with the WP29/EDPB Guidelines. This will allow data controllers to leverage DPIAs to their utmost benefit and in the most effective manner by focusing on the development of high quality assessments for processing activities that truly present a high risk. However, at this stage, a review of some DPAs' public lists raises concerns that could impede these goals:

- Some lists have been sent to the EDPB without being published for prior consultation;

- Some lists have been made available in local language only;

- Some lists are white or black lists only, while others include both black and white lists;

- While some lists indicate they are in draft form, others do not specify whether they are drafts and could be interpreted to be final.

It would be helpful if DPAs provided information regarding the process and timing for finalising the national DPIA lists, including when they have been submitted or are likely to be submitted to the EDPB for approval.

In addition, as shown in Annex 1[12] to this paper (which maps the several DPA national lists against the WP29/EDPB Guidelines and against each other) it appears at this stage that:

- Some lists are not consistent with the criteria defined in the WP29/EDPB Guidelines;

- The lists also differ from each other;

- Some lists partially or fully overlap in terms of substance, but use wording that is inconsistent with the WP29/EDPB Guidelines and with each other;

- Some lists combine and mix separate criteria of the WP29/EDPB list into one criterion;

- Some lists reinstate criteria that were included in the draft WP29/EDPB Guidelines, but which were not retained in the Guidelines as finally adopted[13] (such as international transfers as a factor of high risk);

- Some lists could be interpreted to reflect inconsistencies in what constitutes low risk and high risk processing;

- Some lists acknowledge and endorse the WP29/EDPB high risk criteria, while others do not mention them;

- Some lists contain a list of processing for which DPIAs are required and a separate list of high risk factors with different criteria and none of these lists and criteria are consistent with the WP29/EDPB list;

- Some lists contain new criteria or examples that cannot be related to any of the WP29/EDPB criteria; and

- Some lists mention that they are applicable to both national and cross-border data processing, while other lists do not mention their scope.

It is extremely difficult to have a consolidated view of all the criteria that a company would have to consider when assessing whether a multi-country processing entails high risks. At this stage, it could be anticipated that the currently already high number of different and inconsistent high risk criteria that will have to be considered will only increase once all DPAs have issued their lists.

CIPL's Recommendations

In order to enable the protection of personal data and individuals in a way that is calibrated to the actual risk, organisations need an efficient and pragmatic process that does not unduly strain their resources and impose unnecessary administrative efforts in carrying out DPIAs. A lack of harmonisation and consistency with respect to high risk criteria will create confusion and unwarranted complexity for organisations operating across the EU. This will prevent them from implementing and operationalising an efficient and coherent DPIA process within their organisations. Furthermore, it is difficult to see how a lack of harmonisation and consistency in the criteria of high risk processing will not ultimately undermine comparable and similarly strong protections for citizens across the EU. Finally, such inconsistency may also create issues for DPAs in terms of carrying out their regulatory duties. For example, when considering which

white or black lists to apply in a cross-border enforcement action. Thus, CIPL would like to make the following recommendations for the EDPB to consider when issuing opinions on DPAs' individual lists with a view to enabling greater consistency:

1. DPA lists should **follow the EDPB list** and only depart from it in exceptional cases.

2. **The EDPB should assess local lists on the basis of the criteria of proportionality, in line with the "rule of reason" case law** of the Court of Justice in the internal market. Where national lists contain additional criteria compared to the EDPB list, DPAs should be asked to justify why these criteria are appropriate to protect the rights of individuals and why the intended aim cannot be achieved by following the criteria already included in the GDPR or adopted by the EDPB.

3. DPA lists should **employ the EDPB "nomenclature"** or wording to promote clarity, consistency and better understanding by organisations.

4. Factors that were **removed from the draft EDPB guidelines should not be reinstated** at the national level. Thus, factors such as "ex-EEA data transfers depending on the envisaged country of destination and the possibility of further onward transfers" or "cross-border data transfers outside the European Union" should not be permitted.[14]

5. The EDPB should confirm that in situations of cross-border processing, organisations should be allowed to rely on their **lead authority high-risk criteria rather than on local DPA lists for any processing covering more than one EU country**.

6. To enable **consistency of processing activities**, Article 35(6) GDPR should be understood as encompassing all "cross-border activities" as defined under Article 4(23) GDPR. This will capture not only processing activities of companies offering services in several countries, but also processing activities of companies with establishments in more than one Member State.[15]

7. There should be a preference for fewer numbers of high-quality **DPIAs on the basis of the EDPB criteria** rather than large numbers of DPIAs on the basis of differing national criteria. Reserving DPIAs for processing activities that truly present a high risk will enable higher quality and articulated risk-assessments versus a plethora of potentially downgraded risk assessments completed by companies in a more "industrialised" fashion.

8. The EDPB should confirm that in cases of residual risk, after a DPIA has been performed for a multi-country processing, only the **lead authority** of the data controller should have to be consulted, in accordance with Article 36.

Conclusion

We hope the above recommendations provide useful input into issuing opinions on the national DPAs draft lists. CIPL appreciates the EDPB's work in this area and is looking forward to continued dialogue between the EDPB, individual DPAs and organisations on these issues.

If you would like to discuss this paper 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.

References

[1] Pursuant to Article 35(6), the consistency mechanism shall apply where such lists involve processing activities related to the offering of goods or services to data subjects or to the monitoring of their behaviour in several Member States or may substantially affect the free movement of personal data within the Union.

[2] Pursuant to Article 64, the EDPB shall issue an opinion when a DPA aims to adopt a list of the processing operations subject to the requirement for a data protection impact assessment pursuant to Article 35(4).

[3] 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 63 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.

[4] See (a) UK Information Commissioner's Office, Data Protection Impact Assessments, 14 May 2018, available at http://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/;

(b) Irish Data Protection Commission, Data Protection Impact Assessment list for public consultation, available at https://www.dataprotection.ie/docimages/documents/DPIA%20DPC.pdf;

(c) Belgian Privacy Commission, Recommendation on Data Protection Impact Assessments and prior consultation (Recommandation d'initiative concernant l'analyse d'impact relative à la protection des données et la consultation préalable), 28 February 2018, available at https://www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/recommandation_01_2018.pdf;

(d) Polish Data Protection Authority (Generalny Inspektor Ochrony Danych Osobowych (GIODO)), Proposed list of processing for which an Data Protection Impact Assessment is required (Proponowany wykaz rodzajów przetwarzania, dla których wymagane jest przeprowadzenie oceny skutków), available at https://www.giodo.gov.pl/pl/file/13366;

(e) German Federal Commissioner for Data Protection and Freedom of Information (Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI)), Liste von Verarbeitungsvorgängen gemäß Artikel 35 Abs. 4 DSGVO), available at https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Datenschutz/Liste_Verarbeitungsvorgaenge.pdf?__blob=publicationFile&v=2; DPAs of several individual German states (Länder) have also released lists where a DPIA is required. These include:
(i) Baden-Wüerttemberg, available at https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2018/05/Liste-von-Verarbeitungsvorg%C3%A4ngen-nach-Art.-35-Abs.-4-DS-GVO-LfDI-BW.pdf;
(ii) Berlin, available at https://www.datenschutz-berlin.de/pdf/datenschutzfolgeabschaetzung/dsfolge_oeffentlich.pdf;
(iii) Brandenburg, available at https://www.lda.brandenburg.de/media_fast/4055/DSFA_Muss-Liste_oeffentlich_180525.pdf;

(iv) Hamburg, available at https://datenschutz-hamburg.de/assets/pdf/Liste%20Art%2035-4%20DSGVO%20HmbBfDI-%C3%B6ffentlicher%20Bereich_v1.0.pdf;
(v) Lower Saxony, available at https://www.lfd.niedersachsen.de/startseite/datenschutzreform/dsgvo/liste_von_verarbeitungsvorgaengen_nach_art_35_abs_4_dsgvo/liste-von-verarbeitungsvorgaengen-nach-art-35-abs-4-ds-gvo-164661.html;
(vi) Rhineland-Palatinate, available at https://www.datenschutz.rlp.de/fileadmin/lfdi/Dokumente/Orientierungshilfen/DSFA_-_Muss-Liste_RLP_NOE.pdf;
(vii) Thuringia, available at https://www.tlfdi.de/mam/tlfdi/datenschutz/dsfa_muss-liste_04_07_18.pdf;
(viii) Saarland, available at https://datenschutz.saarland.de/fileadmin/datenschutz/ds-gvo/ds-folgenabschaetzung/DSFA_Muss-Liste_DSK_1_0.pdf; and
(ix) Schleswig-Holstein, available at https://www.datenschutzzentrum.de/uploads/datenschutzfolgenabschaetzung/20180525_LfD-SH_DSFA_Muss-Liste_V1.0.pdf;

(f) Dutch Data Protection Authority (Autoriteit Persoonsgegevens), List of types of processing for which a DPIA is mandatory (Wat zijn de criteria van de AP voor een verplichte DPIA?), available at https://www.autoriteitpersoonsgegevens.nl/nl/zelf-doen/data-protection-impact-assessment-dpia;

(g) Spanish Data Protection Authority (Agencia Española de Protección de Datos), Practical Guide for Data Protection Impact Assessments under the GDPR (Guía práctica para Las Evaluaciones de Impacto en la Protección de Los datos sujetas al RGPD), available at https://www.aepd.es/media/guias/guia-evaluaciones-de-impacto-rgpd.pdf.

[5] These additional comments are presented as part of CIPL's GDPR Project, a multiyear project launched in March 2016 that aims to establish a forum for dialogue amongst industry representatives, the EU DPAs, the European Data Protection Supervisor, the European Commission, the ministries of the Member States and academics on the consistent interpretation and implementation of the GDPR through a series of workshops, webinars, white papers and comments.

[6] See CIPL's white paper on Risk, High Risk, Risk Assessments and Data Protection Impact Assessments under the GDPR, 21 December 2016, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_gdpr_project_risk_white_paper_21_december_2016.pdf.

[7] 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, 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.

[8] Comments by the Centre for Information Policy Leadership on the UK ICO Consultation on GDPR DPIA Guidance, 12 April 2018, available at http://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_response_to_ico_gdpr_dpia_guidance-c.pdf.

[9] Comments by the Centre for Information Policy Leadership on the Irish Data Protection Commission Consultation on a Draft List of types of Data Processing Operations which Require a Data Protection Impact Assessment, 4 July 2018, available at

http://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_response_-_irish_dpc_consultation_on_dpia__4_july_2018_-c.pdf.

[10] WP29 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 WP248 rev. 01, available at http://ec.europa.eu/newsroom/document.cfm?doc_id=47711.

[11] *Id.* at pages 4 and 19.

[12] Annex 1 comprises of a mapping of available DPA black lists against the EDPB high risk criteria contained in its Guidelines on DPIA (See *Supra* note 10). Annex 1 does not include an entry for Germany but it is important to highlight that given that Germany is made up of several states (Länder), there are several black lists from national DPAs at the state level in Germany alone. Currently nine out of sixteen DPAs in Germany have produced such ancillary DPIA lists. This will create more divergence not only between Germany and other Member States at the EU level but between the different German states at the regional level.

[13] Compare *Supra* note 10 at page 9-11 with Consultation version of WP248, available at https://ec.europa.eu/newsroom/document.cfm?doc_id=44137 at page 7-9.

[14] As stated by CIPL in its response to the Irish Data Protection Commission's Consultation on DPIA (*Supra* note 9) 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 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/EDPB.

[15] See Article 4(23) GDPR on the definition of cross-border processing.

ANNEX 1

Annex 1: DPA Lists of High Risk Processing Mapped to EDPB High Risk Criteria Contained in its Guidelines on DPIA and determining whether processing is "likely to result in high risk" for the purpose of the GDPR (http://ec.europa.eu/newsroom/document.cfm?doc_id=47711)

UK Information Commissioner's Office, Data Protection Impact Assessments, 14 May 2018, available at http://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/

UNITED KINGDOM

Guidance applies to data processing carried out by UK organisations.

		ICO LIST OF PROCESSING REQUIRING A DPIA MAY 2018										UK REFERS TO THE EDPB GUIDELINES								
		1. Use of new technologies	2. Use of profiling or special category of data to decide on access to services	3. Profiling individuals on a large scale	4. Any processing of biometric data	5. Any processing genetic data other than by an individual GP or health professional	6. Match data or combine datasets from different sources	7. Collect personal data from a source other than the individual without providing them with a privacy notice	8. Track individuals' location or behaviour	9. Profile children or target marketing or online services at them	10. Process personal data that might endanger the individual's physical health or safety in the event of a security breach	1. Evaluation or scoring	2. Automated decision-making with legal or similarly significant effects	3. Systematic monitoring	4. Sensitive data or data of a highly personal nature	5. Data processed on a large scale	6. Matching or combining datasets	7. Data concerning vulnerable data subjects	8. Innovative use or applying new technological or organisational solutions	9. Preventing data subjects from exercising a right or using a service or contract
FINAL EDPB LIST OCT 2017	1. Evaluation or Scoring (including profiling and predicting)		X	X				NEW		X		X								
	2. Automated Decision-making producing legal or similarly significant effects												X							
	3. Systematic monitoring								X					X						
	4. Sensitive data or data of a highly personal nature		X		X	X					X				X					
	5. Data processed on a large scale			X												X				
	6. Matching or combining datasets						X										X			
	7. Data concerning vulnerable data subjects									X								X		
	8. Innovative use or applying new technological or organisational solutions	X																	X	
	9. Processing itself prevents exercise of a right or use of service or contract		X																	X
DRAFT EDPB LIST APRIL 2017	10. Data transfer across borders outside the European Union																			

Irish Data Protection Commission, Data Protection Impact Assessment list for public consultation, available at https://www.dataprotection.ie/docimages/documents/DPIA%20DPC.pdf

IRELAND

Guidance applies to both national and cross-border data processing.

		IRELAND DRAFT LIST OF PROCESSING REQUIRING A DPIA											IRELAND DRAFT LIST OF FACTORS THAT CAN LEAD TO HIGH RISK PROCESSING									
		1. Use of personal data on a large-scale for a purpose other than initial collection	2. Profile vulnerable persons, including children to target marketing or online services	3. Use profiling or special category data to determine access to services	4. Monitor, track or observe individual location or behaviour	5. Profile individuals on a large scale	6. Process biometric data to identify an individual	7. Process genetic data	8. Indirectly source personal data where GDPR transparency requirements not met	9. Combine, link or cross-reference separate datasets to contribute to profiling or behavioral analysis	10. Process personal data based on legislative measure under local data protection Act	11. Further process data for archiving purposes in the public interest, scientific or historical research or statistical purposes	1. Uses of new or novel technologies	2. Data processing at a large scale	3. Profiling, Evaluating, Scoring individual behaviour	4. Systematic monitoring, observation or control of individuals, including in a public area	5. Processing of sensitive data and location, financial and electronic communication data	6. Processing of combined data sets beyond expectation of individual	7. Processing of data of vulnerable individuals	8. Ex-EEA transfers depending on destination and possibility of onward transfers	9. Automated decision making with legal or significant effects	10. Insufficient protection against unauthorized reversal of pseudonymisation
FINAL EDPB LIST OCT 2017	1. Evaluation or Scoring (including profiling and predicting)		X	X		X			NEW	X	NEW	NEW			X							NEW
	2. Automated Decision-making producing legal or similarly significant effects																				X	
	3. Systematic monitoring				X											X						
	4. Sensitive data or data of a highly personal nature			X			X	X									X					
	5. Data processed on a large scale	X				X								X								
	6. Matching or combining datasets									X								X				
	7. Data concerning vulnerable data subjects		X																X			
	8. Innovative use or applying new technological or organisational solutions												X									
	9. Processing itself prevents exercise of a right or use of service or contract			X																		
DRAFT EDPB LIST APRIL 2017	10. Data transfer across borders outside the European Union																			X		

Belgian Privacy Commission, Recommendation on Data Protection Impact Assessments and prior consultation (Recommandation d'initiative concernant l'analyse d'impact relative à la protection des données et la consultation préalable), 28 February 2018, available at https://www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/recommandation_01_2018.pdf

BELGIUM

Unclear whether guidance applies to only national or cross-border data processing as well

		BELGIAN DPA DRAFT LIST OF PROCESSING REQUIRING A DPIA										BELGIUM REFERS TO THE EDPB GUIDELINES								
		1. Processing of biometric data for the purpose of identifying individuals in a public area or in a private area accessible to the public	2. Collecting personal data from third parties for the purpose of making decisions to refuse or terminate a service contract with an individual	3. Further processing of special category data except where the controller obtains consent or the processing is necessary for the controller to meet its legal obligations	4. Where the processing involves use of a medical implant and a data breach could compromise the physical health of the individual	5. Large scale processing of personal data from vulnerable individuals for a purpose other than which the data was collected	6. Where data is collected on a large scale from third parties for profiling purposes	7. Where special category data or data of a very personal nature are systematically exchanged between multiple controllers	8. Large scale processing of device generated data equipped with sensors for profiling purposes	9. Large scale and/or systematic processing of telephony data, internet data or other communication data, metadata, location data, or data which permits the organisation to locate individuals where the processing is not strictly necessary for the service requested by the data subject	10. Large scale processing of personal data where individuals' behaviour is observed, collected, established or influenced in a systematic manner and using automated means, including for advertising purposes	1. Evaluation or scoring	2. Automated decision-making with legal or similarly significant effects	3. Systematic monitoring	4. Sensitive data or data of a highly personal nature	5. Data processed on a large scale	6. Matching or combining datasets	7. Data concerning vulnerable data subjects	8. Innovative use or applying new technological or organisational solutions	9. Preventing data subjects from exercising a right or using a service or contract
FINAL EDPB LIST OCT 2017	1. Evaluation or Scoring (including profiling and predicting)						X		X			X								
	2. Automated Decision-making producing legal or similarly significant effects										X		X							
	3. Systematic monitoring									X	X			X						
	4. Sensitive data or data of a highly personal nature	X		X	X			X							X					
	5. Data processed on a large scale					X	X		X	X	X					X				
	6. Matching or combining datasets							X									X			
	7. Data concerning vulnerable data subjects					X												X		
	8. Innovative use or applying new technological or organisational solutions								X										X	
	9. Processing itself prevents exercise of a right or use of service or contract		X																	X
DRAFT EDPB LIST APRIL 2017	10. Data transfer across borders outside the European Union																			

Polish Data Protection Authority (Generalny Inspektor Ochrony Danych Osobowych (GIODO)), Proposed list of processing for which an Data Protection Impact Assessment is required (Proponowany wykaz rodzajów przetwarzania, dla których wymagane jest przeprowadzenie oceny skutków), available at https://www.giodo.gov.pl/pl/file/13366

POLAND

Guidance applies to companies with Polish operations only.

POLISH DRAFT LIST OF PROCESSING REQUIRING A DPIA APRIL 2018

		1. Evaluation or assessment, including profiling and prediction for purposes that may have negative legal, physical, financial or other effects on natural persons	2. Automated decision making that produces legal, financial or similar material results	3. Systematic large scale monitoring of publicly accessible places using elements of recognition of features or properties of objects occurring in the monitored space (not including video monitoring for use of law infringement incidents)	4. Processing of special categories of personal data concerning convictions and law infringements	5. Large scale data processing, where the concept of large scale concerns: the number of people whose data is processed, scope of processing, data retention period and geographical scope of processing	6. Performing comparisons, assessment of or drawing conclusions based on the analysis of data obtained from various sources	7. Processing data concerning persons whose assessment and the services they are provided with depend on entities or persons which have authoritative and/or assessment-related powers	8. Innovative use or application of technological or organisational solutions	9. Cross-border data transfers outside the EU	10. When the data processing in itself prevents data subjects from exercising their rights or using a service or a contract
FINAL EDPB LIST OCT 2017	1. Evaluation or Scoring (including profiling and predicting)	X					X				
	2. Automated Decision-making producing legal or similarly significant effects		X								
	3. Systematic monitoring			X							
	4. Sensitive data or data of a highly personal nature				X						
	5. Data processed on a large scale			X		X					
	6. Matching or combining datasets						X				
	7. Data concerning vulnerable data subjects							X			
	8. Innovative use or applying new technological or organisational solutions								X		
	9. Processing itself prevents exercise of a right or use of service or contract										X
DRAFT EDPB LIST APRIL 2017	10. Data transfer across borders outside the European Union									X	

Dutch Data Protection Authority (Autoriteit Persoonsgegevens), List of types of processing for which a DPIA is mandatory (Wat zijn de criteria van de AP voor een verplichte DPIA?), available at https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/data-protection-impact-assessment-dpia#wat-zijn-de-criteria-van-de-ap-voor-een-verplichte-dpia-6667

NETHERLANDS

Guidance applies to Dutch companies

		DUTCH DPA LIST OF PROCESSING REQUIRING A DPIA															NETHERLANDS REFERS TO THE EDPB GUIDELINES								
		1. Secret investigation	2. Black lists	3. Fight against fraud	4. Credit scores	5. Financial situation	6. Genetic personal data	7. Health data - excluding doctors and individual health care professionals	8. Partnerships	9. Camera surveillance	10. Flexible camera surveillance (i.e., cameras on clothing or helmets or dashcams)	11. Control employees	12. Location data	13. Communication data	14. Internet of Things	15. Profiling	16. Observing and influencing behaviour	1. Evaluation or scoring	2. Automated decision-making with legal or similarly significant effects	3. Systematic monitoring	4. Sensitive data or data of a highly personal nature	5. Data processed on a large scale	6. Matching or combining datasets	7. Data concerning vulnerable data subjects	8. Innovative use or applying new technological or organisational solutions	9. Preventing data subjects from exercising a right or using a service or contract
FINAL EDPB LIST OCT 2017	1. Evaluation or Scoring (including profiling and predicting)	NEW			X				NEW							X		X								
	2. Automated Decision-making producing legal or similarly significant effects															X	X		X							
	3. Systematic monitoring							X		X	X						X			X						
	4. Sensitive data or data of a highly personal nature			X		X	X									X					X					
	5. Data processed on a large scale												X	X	X		X					X				
	6. Matching or combining datasets																						X			
	7. Data concerning vulnerable data subjects											X												X		
	8. Innovative use or applying new technological or organisational solutions													X	X										X	
	9. Processing itself prevents exercise of a right or use of service or contract		X																							X
DRAFT EDPB LIST APRIL 2017	10. Data transfer across borders outside the European Union																									

Spanish Data Protection Authority (Agencia Española de Protección de Datos), Practical Guide for Data Protection Impact Assessments under the GDPR (Guía práctica para Las Evaluaciones de Impacto en la Protección de Los datos sujetas al RGPD), available at https://www.aepd.es/media/guias/guia-evaluaciones-de-impacto-rgpd.pdf

SPAIN

	Guidance applies to cross-border data processing	AEPD LIST OF PROCESSING REQUIRING A DPIA					SPAIN REFERS TO THE EDPB GUIDELINES								
		1. The technologies (cloud, databases, servers), applications, devices and/or techniques used for processing personal data	2. The classification of their database through typologies (e.g., human resources, marketing, children, data concerning health and/or filing system), purposes of the processing, or level of sensitivity, value and criticality of the data	3. The data lifecycle, similar processing operations that present similar risks and risks by defect	4. The individuals who can access or use personal data, such as data processors, third parties, recipients or employees	5. Potential harms associated with the processing activity and potential negative impacts on data subject rights that could result from a data breach if it materializes	1. Evaluation or scoring	2. Automated decision-making with legal or similarly significant effects	3. Systematic monitoring	4. Sensitive data or data of a highly personal nature	5. Data processed on a large scale	6. Matching or combining datasets	7. Data concerning vulnerable data subjects	8. Innovative use or applying new technological or organisational solutions	9. Preventing data subjects from exercising a right or using a service or contract
FINAL EDPB LIST OCT 2017	1. Evaluation or Scoring (including profiling and predicting)			NEW	NEW		X								
	2. Automated Decision-making producing legal or similarly significant effects							X							
	3. Systematic monitoring								X						
	4. Sensitive data or data of a highly personal nature		X			X				X					
	5. Data processed on a large scale										X				
	6. Matching or combining datasets											X			
	7. Data concerning vulnerable data subjects												X		
	8. Innovative use or applying new technological or organisational solutions	X												X	
	9. Processing itself prevents exercise of a right or use of service or contract														X
DRAFT EDPB LIST APRIL 2017	10. Data transfer across borders outside the European Union														

ANNEX 2

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.

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.