Centre for Information Policy Leadership
Hunton & Williams LLP

19 May 2017

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"
adopted on 4 April 2017

On 4 April 2017, the Article 29 Data Protection Working Party (WP29 or WP) adopted its "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" (Guidelines). The WP invited public comment on these documents by 23 May 2017. The Centre for Information Policy Leadership (CIPL) welcomes the opportunity to submit the below brief comments. These additional comments follow up on CIPL's 21 December 2016 white paper on "Risk, High Risk, Risk Assessments and Data Protection Impact Assessments under the GDPR"[1] (CIPL White Paper), which CIPL had submitted to the WP29 as formal initial input to the WP's development of DPIAs and "high risk" guidance.[2]

As a general matter, CIPL appreciates the WP's pragmatic and restrained approach to its implementation guidance on DPIAs and "high risk". More specifically, CIPL welcomes:

- The WP's recognition of the notion that DPIAs, risk assessments and the notion of "high risk" are context-specific and that organisations must have flexibility to devise risk assessment frameworks and methodologies that are appropriate to them.
- The WP's acknowledgement that a single DPIA can be used to assess multiple processing operations that present similar risks.
- The inclusion in the Guidelines of criteria and examples for identifying "high risk" as opposed to a fixed list of high-risk processing activities that may include processing that, in fact, may not be "high risk" in some contexts and that would quickly become outdated based on changed circumstances.
- Qualifying prior consultation with DPAs under Article 26 GDPR as exceptional and left for cases where the residual risk is high and the data controller acknowledges that it cannot be mitigated.

CIPL also has a number of specific comments and recommendations for improving the WP's DPIA Guidelines, as further set forth below.

---

[1] https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_gdpr_project_risk_white_paper_21_december_2016.pdf.

[2] These additional comments are presented as part of the CIPL 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.

Comments and Recommendations

1. What does a DPIA address? A single processing operation or a set of similar processing operations? (Section III. A., p. 6)

Processing by joint controllers. The WP states that "when the processing operation involves joint controllers, they need to define their respective obligations precisely. Their DPIA should set out which party is responsible for the various measures designed to treat risks and to protect the rights of the data subjects." In general, we welcome that the WP addresses DPIAs in the context of joint controller relationships. The Guidelines should acknowledge that such joint DPIAs in the context of joint controller relationships may raise trade secret, confidentiality or security concerns.

Recommendation: Clarify that where there are joint controller relationships, a joint controller may define its role with respect to the processing without revealing through a DPIA any trade secrets, intellectual property or privileged or confidential information.

DPIA of provider of technology may inform DPIA of user of technology. The Guidelines state that DPIAs can be useful for assessing a technology product that is "likely to be used by different data controllers to carry out different processing operations." According to the WP, while each data controller using the product must carry out its own DPIA for its specific purpose, these DPIAs may be informed by a DPIA prepared by the provider (manufacturer or creator/designer) of the product. However, we note that such providers of technology may not be "controllers" and thus may be under no obligation to conduct a DPIA. If they did conduct a DPIA, providing this DPIA to a controller using their technology may raise security risks for the provider and the possibility of disclosing trade secrets.[3]

In addition, the provider of technology may also be the processor for the controller to whom the technology has been provided. In that case, any obligations the provider/processor may have with respect to DPIAs are described in Article 28(f), requiring the processor to "assist" the controller, including with respect to the controller's DPIA obligations, "taking into account … the information available to the processor." Presumably, this could mean that the provider/processor may share any DPIA it may have about its technology (or appropriate elements of such DPIA) with the controller for purposes of informing the controller's DPIA. If the provider/processor has not produced a DPIA for a new technology, Article 28(f) would still require the provider/processor to "assist" the controller in other ways with the controller's DPIA. This should be explained in the Guidelines.

Recommendation: Clarify that when sharing a DPIA with the user/deployer of a technology, the provider (manufacturer/creator) of the technology may limit what it shares to protect its intellectual property and to avoid security risks. The obligations of the manufacturer/creator who also is a processor should also be explained in accordance with Article 28(f).

"Similar processing". The WP provides a narrow definition of 'similar processing': "This might mean where similar technology is used to collect the same sort of data for the same purposes. For example, a

[3] This was correctly recognised by the WP in a similar context in its discussion about whether DPIAs should be published (see Guidelines, p. 17).

group of municipal authorities that are each setting up a similar CCTV system could carry out a single DPIA covering the processing by these separate controllers, or a railway operator (single controller) could cover video surveillance in all its train stations with one DPIA." There are some instances where a controller may be implementing similar features or running similar software across different products, such that part of the processing for the whole product may already be covered under an existing DPIA. Furthermore, for existing products that may undergo multiple iterations, the WP should clarify that an existing DPIA could be relied upon and updated to address any new risks.

Recommendation: Clarify that for new implementations of a similar feature or software (constituting part of a new product), even across different products or newer versions of existing products, controllers may rely on existing DPIAs for the similar feature or software used.

2. When is a DPIA mandatory? Where a processing is "likely to result in high risk". (Section III.B.a, pp. 7-11)

DPIAs for new technology. The WP notes that the DPIA requirement for "high risk" processing is "particularly relevant when a new data processing technology is being introduced." However, it is important to acknowledge also that in many contexts such new technology may not pose a high risk or require a DPIA. Thus, the Guidelines should confirm that using new technology in and of itself should not be viewed as a sufficient trigger for likely high-risk status requiring a DPIA. Instead, whether a DPIA is required depends on the technology itself and any high-risk characteristics based on context, scope and purpose of the intended processing.

Recommendation: Acknowledge in the Guidelines that new technology may not necessarily in itself pose a high risk or require a DPIA and that any high risk must be established in conjunction with contextual factors, such as scope and purpose of processing. The fact that technology is "new" is only one factor for determining the level of risk related to the processing.

Conducting a DPIA where it is not clear that a DPIA is required. The WP also recommends that in cases where it is not clear that a DPIA may be required, a DPIA be carried out nonetheless, as it is a "useful tool" to determine high risk. While we agree that organisations must always consider risk with respect to all their processing, including for purposes of determining whether there is a "high risk" that merits a full DPIA, we suggest that in many cases this may not have to involve a full-blown DPIA. Organisations should be able to conduct an initial risk assessment and triage based on certain criteria and red flags that help establish the need for a full DPIA under GDPR.

More in general, we suggest that because of the DPIA's status as a specific accountability tool for "high risk" processing, it would make sense from a policy perspective to limit its use to that purpose, rather than dilute its special role through a broader use in situations where it is not strictly required. A DPIA is only one of the accountability tools that have to be implemented under the GDPR and, together with other compliance steps, contributes to effective data protection for individuals. Companies are also appointing DPOs, setting up governance structures, performing data mapping, implementing BCR and conducting risk assessments short of a formal DPIA. Creating an expectation of a full-blown DPIA in most circumstances may undermine the effective broader implementation of the GDPR, particularly for SMEs.

Recommendation: Clarify that an initial risk assessment short of a full-blown DPIA may be sufficient to determine whether there is likely high risk. If there is likely high risk, the organisation can proceed to conduct a DPIA. Confirm that a DPIA is an exceptional and formal tool under the GDPR that needs to be performed only for likely high-risk processing and that it is part of a larger compliance structure under the GDPR that includes many other elements.

Lists of the kind of processing that require a DPIA. We welcome that the WP provided criteria and examples for determining likely high-risk processing rather than provide a definitive list of specific activities. Given that all data processing operations and any associated risks are highly context-specific and linked to the purpose of processing, it would be unhelpful to categorise specific processing activities as "high risk" and itemise them on a list. Such lists would also risk being outdated quickly and could lead to inconsistencies between EU member states.

However, the WP may have left the door open for national DPAs to develop lists with "more specific content" that may go beyond criteria and examples (Guidelines at 10). We recall that under Article 35(4), supervisory authorities must establish "a list of the kind of processing operations", not a list of specific processing operations.[4] This is a significant distinction. The quoted text in the Guidelines would seem to allow the listing of specific processing activities, which may result in rigid and inflexible lists of activities that must be treated as "high risk" but that may, in fact, not be "high risk" in particular contexts or may be no longer high risk due to positive technological solutions. In contrast, the text of the GDPR suggests a listing of criteria and examples, which have to be considered and applied in context. In fact, this is what the WP itself has done in the Guidelines by providing only criteria and examples.

Finally, the WP should also encourage a harmonised approach to creation of additional national lists of the criteria and examples. National divergences in setting criteria for DPIAs would be detrimental to the harmonised implementation of the GDPR and smooth functioning of the Digital Single Market.

Recommendation: **Correctly quote the GDPR (i.e. lists of the kind of processing) and clarify that to the extent "high risk" lists by national supervisory authorities are created, they, too, should include only criteria and examples that must be evaluated for actual "high risk" on a case-by-case basis. Encourage a harmonised approach to the creation of additional national lists of criteria and examples.**

Criteria for "high risk" processing. As noted above, the WP also set forth a list of criteria for determining "high-risk" activities, above and beyond the examples set forth in Article 35(3). We have some specific concerns with respect to several of the criteria listed by the WP:

- **Evaluation or scoring.** The criterion of "evaluation or scoring" refers to GDPR Recitals 71 and 91, but significantly broadens their scope: Recital 71 addresses profiling concerning "personal preferences or interests, reliability or behaviour, location or movements" *only* insofar as it may produce legal effects or significantly affect individuals. The WP's example of marketing profiles based on usage or navigation on a website does not fit into this category. While evaluations or scoring (or automated decisions) impacting employment, insurance or credit eligibility would

[4] Article 64(1) does refer to "a list of the processing operations" but then adds that they must be pursuant to Article 35(4), which refers to "a list of the kind of processing."

create such legal effects, it is a significantly broader assertion for the WP to state that any behavioural or marketing profiles based on website navigation by default carry such a risk and produce legal effect or similarly significantly affect individuals.

- **Automated decision-making with legal or similar significant effect.** The WP refers to Article 35(3), which indicates that processing likely to result in high risk could include "a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person." (Emphasis added). It is clear from the text that the legislators intended this to cover profiling-type activities where decisions produce legal effects or similarly significant effects—not "normal" profiling where there are no such effects. The legislators' intention was clear and logical: "normal" profiling is not likely to result in high risks to individuals. Therefore, the criterion of "evaluation or scoring" should be clarified to that effect. In addition, the criterion of "automated decision-making" should make clear that "similarly significant effects" are those which create material, adverse impact on the individuals—in other words, that there is an equivalent level of disruption to when a legal right has been denied to the individual.

Recommendation: Clarify that there must be legal effects or substantially similar effects in connection with "evaluation and scoring" and "automated decision-making" and that substantially similar effects are those that create an equivalent material adverse impact on the individual. The example of marketing profiles based on usage or navigation on a website should be removed from the evaluation or scoring criterion.

- **Sensitive data.** The definition of sensitive data under Article 9 of the GDPR should be identical in all EU countries. However, Article 9 provides the member states with competences for specifications and, currently, EU countries have their own lists that are not completely consistent with each another (e.g. France includes social security numbers [which, however, is consistent with Article 87 on the processing of national identification numbers]; the Netherlands includes financial data). Notwithstanding their legality under the GDPR, if such differences persist, they will have significant practical compliance implications. Organisations would have to conduct multiple DPIAs for the same processing operations and/or DPIAs for some member states but not for others, based on the same processing. As a result, this issue should be highlighted in the Guidelines to encourage member states to minimise such differences.

  Also, the WP indicates that DPIAs may be necessary for processing of other data that is not defined as sensitive, but may be of a sensitive nature and hence merit a DPIA, such as electronic communication data, location data and financial data. It is important to underline that GDPR Article 9 provides an exhaustive list of the types of data considered to be special categories requiring additional protection; these do not include electronic communications data, location data or financial data. We find this distinction between the categories listed in Article 9 and other types of data that may be of a sensitive nature difficult to apply in practice and do not believe that DPIAs are necessary just because location or financial data are processed. We strongly recommend that the WP limit the scope of sensitive data to the categories listed in

Article 9 and the criminal data to which it refers, if only to provide greater clarity and consistency for controllers.

Finally, data that would allow probabilistic inferences of sensitive data, but which may not itself be sensitive data should not be covered under this DPIA requirement. For example, information voluntarily posted online by users in free-form text may reveal their political or religious beliefs. An online service provider should not be required to conduct a DPIA simply because individuals arbitrarily include information revealing political or religious beliefs.

Recommendation: References to "sensitive data" should be limited to the data categories listed in Article 9 and personal data relating to criminal convictions and offenses. Clarify that DPIA requirements for the processing of sensitive data should apply only where there is a product designed to collect or process sensitive data, or where the controller has knowledge that sensitive data is being collected on a large scale, and not merely incidentally.

- **Data concerning vulnerable data subjects.** This includes the example of employees. However, human resources management involves many legitimate and common processing activities with respect to employee data where employees should not be considered vulnerable data subjects. Considering the processing of employee data by default potentially "high risk" on the basis that employees are "vulnerable" would require every organisation to conduct huge numbers of DPIAs for common and expected data processing for HR management. This would not only be impracticable, it would be unnecessary due to the absence of risks and harms to individuals. We recommend the WP to be more specific, or even delete the example of employees as being by default considered vulnerable data subjects.

- **A second concern relates to children's data.** In suggesting a DPIA where children's data is concerned, the WP indicates this may be appropriate as "children can be considered as not able to knowingly and thoughtfully oppose or consent to the processing of their data." Article 8 clearly indicates that children above the relevant legal age (or the guardians for those below the legal age) can consent to the processing of their data, as long as the form and method of consent comports with the consent requirements in Article 6. Either the controller has validly obtained consent from a child (or his or her guardian), or it has not. A DPIA will not be able to compensate for invalid consent. We recommend the WP remove this example.

Recommendation: Clarify that employees should be treated as vulnerable persons only in well-defined circumstances in which the purposes and contexts of the processing may make them more vulnerable, such as when employers process employee personal data outside of the legitimate scope of HR management, or when imbalance is created in relation to processing of employees' special categories of data, as defined by Article 9.[5] Reconsider the reference to consent in respect to children.

- **Cross-border transfers.** The criterion of "data transfer across borders outside the European Union" is problematic. Recital 116 only refers to "increased risk", which is different from "high

[5] See also Recital 48, recognising that the processing of employee personal data within a group is a legitimate interest of the data controller.

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 companies, transfers outside the EU 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". Finally, none of the articles of Chapter 5 mention the need to perform any DPIA or the notion of high risk.

Recommendation: **The criterion of cross-border transfers for determining "high risk" should not be included in the Guidelines. Alternatively, the relevance of this criterion should be limited to certain limited transfers pursuant to Article 49 (derogations for specific situations) where the transfer is necessary for the purposes of compelling legitimate interests. (Art. 49(1) (final paragraph)).**

- **Large-scale data sets.** The WP's inclusion of "large-scale" processing as separate criterion for determining "likely high risk" goes beyond the GDPR and creates uncertainty for data controllers. Article 35(3)(c) couples "large scale" with the processing of special categories of data and/or data relating to criminal convictions and offences. It does not treat "large scale" as a separate likely high-risk criterion. Treating it as a separate criterion may have the effect of setting aside the risk-based approach introduced by lawmakers in the GDPR and opens the door to treating any such processing as likely high risk even if there is no actual risk to individuals.

- **Data sets that have been matched or combined.** Similarly, such data sets should also not be considered per se and on their own as "likely high risk", for the same reasons stated above in connection with "large scale". Also, matching and combining data sets is not mentioned in Article 35(3).

Recommendation: We recommend reconsideration of "data processed on a large scale" and "data sets that have been matched or combined" as criteria for identifying likely "high risk" as they will have the effect of causing the conduct of a large number of unnecessary DPIAs based solely on these criteria. This will detract from conducting DPIAs where they are actually warranted. Alternatively, consistent with Article 35(3)(c) and Recital 91, clarify that "large scale" is not an independent criterion that can be assessed separately from context and additional factors.

Other elements to consider in the assessment of the risk

1. Balance between harms and benefits. The GDPR makes clear that the likelihood and severity of the risk should be determined by reference to the nature, scope, context and purpose of the processing and that the assessment should be objective (Recital 76). In this context, the WP guidance should address the balance between harms and benefits: the same risk can lead to a different scoring depending on the benefits (high or low) that it may bring to individuals. Benefits should be considered from the very

beginning of the risk assessment. Similarly, "the risk of not engaging in processing" should be part of the assessment.[6]

Recommendation: Include "benefits" in the assessment of the likelihood and severity of the risk.

2. Taking consent into consideration: Consent given by an individual under the conditions of Article 7 GDPR is an indication that he or she is aware and had agreed to the contextual elements of the processing, including the risk element. It should therefore be considered when assessing the risk.[7]

Recommendation: Include consent in the assessment of the likelihood and severity of the risk.

Processing meeting only one "high risk" criterion: The Guidance states that in some cases, a processing meeting only one of the "high risk" criteria identified by the WP will be sufficient to trigger the need for a DPIA. However, the WP does not provide additional elements to identify in what cases one criterion will be sufficient. The Guidance should make clear that such situations are an exception and should provide additional elements to help identify them.

Recommendation: Further specify in what situation one "high risk" criterion is sufficient to require a DPIA.

Two criteria trigger: The WP suggests that "as a rule of thumb … processing operations which meet at least two criteria will require a DPIA" (p. 10). This appears to be a somewhat arbitrary trigger. Instead, we recommend that the WP suggest that data controllers assess the overall severity and impact of the risk(s) involved, rather than focusing on the number of criteria met.

Recommendation: Reconsider the suggestion that meeting two criteria triggers the DPIA obligation. Instead, consider suggesting that based on the criteria listed, controllers assess the overall severity, likelihood and impact of the risks involved and make determination accordingly.

Documenting the reasons for not conducting a DPIA. The WP also states that a controller should "thoroughly document the reasons for not carrying out a DPIA" in cases where there are at least two "high risk" criteria (which, according to the WP may, as a rule of thumb, indicate "high risk"), but the controller nevertheless believes there is no "likely high risk".

We believe that this goes beyond what is required by GDPR, which requires only that DPIAs be documented. The only GDPR requirement that seems relevant is that under Article 24, controllers and processors must be "able to demonstrate" that processing is in accordance with the GDPR. The requirement to "be able to demonstrate" does not necessarily require "thorough documentation", or even a written document, of the reasons not to perform a DPIA, but may be accomplished by other means, such as:

[6] *See also* CIPL White Paper at pp. 7, 38-39.
[7] *See also* CIPL White Paper at p. 11.

- Internal policies or processes in which high-risk and non-high-risk processing are flagged for different treatment or review.
- Having a GDPR certification, marks or seals, or by adherence to a code of conduct (*see* Article 24(3)), or by having BCR or an internal privacy compliance program that define the processes by which organisations must determine likely high risk.
- Meeting the requirements of Article 30 (record of processing activities) when determining the purposes of the processing (30(1)(b), which should serve to demonstrate "due diligence" by the controller in reaching a determination of whether a DPIA is required.
- Having conducted a preliminary risk assessment/triage that demonstrates why no full-blown DPIA was necessary.
- Previous authorisation by a DPA.

Finally, Article 24(2) limits the requirement to implement measures to demonstrate compliance to what is "proportionate" to the processing activities at hand, which may militate against "thoroughly documenting" a decision not to conduct a DPIA in certain cases.

Recommendation: Reconsider this recommendation or clarify the intent of "thoroughly document" in a way that is consistent with the GDPR, acknowledging the range of options available to support a decision not to conduct a DPIA.

3. When isn't a DPIA required? When the processing is not "likely to result in a high risk", or has already been authorised, or has a legal basis. (p. 11)

"Low-Risk" lists. The WP notes that DPIAs are not required where, amongst other cases, the processing activity is included in a list by a DPA of processing activities for which no DPIA is required. We believe that these lists, which are not mandatory under Article 35(5), will be very helpful to provide clarity to organisations and should be consistent across the EU. This is also the purpose of the second sentence of Article 35(5), requiring DPAs to communicate those lists to the EDPB. However, unfortunately, Article 64 GDPR does not mandate the Board to issue an opinion on these lists (contrary to the lists based on Article 35 (4)).

Recommendation: We recommend that the WP call for applying the consistency mechanism to lists of "low-risk processing", clarifying also that no DPIAs will be needed across the EU for any activities itemised on these lists. In addition, we suggest that the WP clearly explain that this list would be nonexclusive and nonexhaustive.

Member state laws that say no DPIA required. The WP also notes that where a processing operation has a legal basis in EU or member state law that "has stated that an initial DPIA does not have to be carried out …" a DPIA is not required. However, the relevant Article 35(10) does not require a statement in such law that no DPIA is required. Instead, the GDPR specifies that when the EU or member state law provides for a legal basis and that a data protection impact assessment has already been carried out as

part of general impact assessment in the context of the adoption of the legal basis, a DPIA will not be necessary unless deemed necessary by the member state.

Recommendation: Reconsider the interpretation of Article 35(10) by not adding additional elements.

4. What about already existing processing operations? DPIAs are needed for those created after May 2018 or that change significantly. (pp. 11-12)

Frequency of DPIAs. The WP recommends that DPIAs should be continuously carried out as a matter of good practice and should be "re-assessed after 3 years, perhaps sooner, depending on the nature of the processing". This goes well beyond Article 35(11) of the GDPR, which only requires a review when necessary.

Each controller should be accountable for determining the re-assessment of a DPIA. The factors that will be taken into consideration by DPAs could be provided as part of the guidance to provide some clarity around the factors DPAs will consider in determining whether the data controller acted in line with the GDPR.

Finally, just as a change in circumstances with respect to processing operations may create a "likely high risk" and, thus, the need for a DPIA, other changes may remove such likelihood of high risk with respect to processing that is currently the subject of a DPIA. The Guidelines might address this scenario and how one might "retire" an existing DPIA.

Recommendation: The WP should not specify a time frame for re-assessments of DPIAs and should leave it to organisations to determine the frequency of re-assessments based on the circumstances and necessity, such as when there is a substantial change to the purpose or nature of the processing. The Guidelines might also address the situation where a change with respect to the processing removes the likely high risk and the need for a DPIA where a DPIA had been previously created.

5. How to carry out a DPIA? (Section III.C., p. 13)

Seeking views of data subjects. Commenting on the requirement that controllers must "seek the views of data subjects or their representatives, where appropriate", the WP lists trade and labor unions as possible interlocutors for this purpose.

CIPL believes that the obligation to seek views where appropriate may impose significant burdens on organisations if "appropriateness" is not narrowly construed. In addition, seeking views from trade unions may implicate local employment laws that are outside the scope of the GDPR. At most, seeking the view of unions should be limited to exceptional cases and to situations where required by local employment laws.

For example, this recommendation might mean that a company's monitoring of its employees access and use of company systems for security purposes could be subject to review by trade unions. This may be problematic for companies to the extent they would have to disclose their security and cybersecurity

plans to trade unions, which is a risk that is specifically identified in Article 35(9) GDPR ("without prejudice to the protection of commercial or public interests or the security of processing operations"). The proposed consultations with trade unions could have the effect of lowering the security level in organisations.

The WP recommends that organisations should document their disagreement with the views of individuals concerned. This requirement could have a counterproductive result in organisations' finding it harder to consult the individuals in the first place. In addition, the interaction with the rules of legal privilege should be considered where advice has been taken from legal counsel—it is unlikely that the organisation would want to disclose such advice.

Also, the recommendation that controllers document the reasons for not seeking the views of data subjects would result in excessive burdens and is not required by the GDPR. For example, there will be many instances where seeking such views will not be appropriate, such as where seeking such views prior to the public release of a product or service may undermine an organisation's commercial secrets and IP rights. Also, some organisations have no direct relationships with individuals. Thus, documenting each decision not to seek such views will result in disproportionate burdens on controllers.

We also note that demonstrating compliance is already part of the accountability requirement of Article 24 and that it should be left to organisations to determine how to demonstrate compliance in respect of the DPIA consultation requirement. As discussed above on pp. 8-9 (documenting the reasons for not conducting a DPIA), the relevant Article 24 requirement to be "able to demonstrate" compliance does not necessarily extend to creating the kind of written documentation described by the WP with respect to decisions not to seek views or disagreement with received views.

Recommendations: **The Guidelines should recognise that (1) "where appropriate" should not be construed too broadly to avoid significant and disproportionate burdens or confidentiality risks on organisations, particularly when it concerns products that have not yet been launched; (2) seeking the views of trade unions should be limited to cases where it is required by local employment laws. The Guidelines should not require organisations to document their reasons for disagreeing with the views of data subjects or for not seeking the views of data subjects.**

6. What is the methodology to carry out a DPIA? Different methodologies but common criteria. (pp. 14-15)

Compliance with a code of conduct. The WP notes that compliance with a code of conduct has to be taken into account when assessing the impact of a processing operation.

Recommendation: We suggest adding GDPR certifications, seals and marks as well as BCR to that statement. They accomplish similar objectives as codes of conduct and similarly provide evidence of an organisation's GDPR compliance and having in place appropriate risk assessment and DPIA processes, as well as mitigations.

Scope of rights to be included. The WP notes that, pursuant to its Statement 14/EN WP 218 (p. 4), "the reference to 'the rights and freedoms' of the data subjects primarily concerns the right to privacy but may also involve other fundamental rights such as freedom of speech, freedom of thought, freedom of movement, prohibition of discrimination, right to liberty, conscience and religion". While controllers should be encouraged to include other rights in their DPIAs, the WP should clarify that the GDPR requires that only *data protection rights* be considered in DPIAs.

Recommendation: Clarify that the GDPR requires only *data protection rights* to be considered in DPIAs.

7. Should the DPIA be published? Yes, either in full or in part, and it must be communicated to the supervisory authority in case of prior consultation. (p. 17)

Publishing the DPIA. While recommending that organisations should consider publishing their DPIAs for a number of reasons, the WP rightly notes that publishing them is not a legal requirement under the GDPR. Publishing a DPIA may either compromise confidential information or intellectual property or impose disproportionate burdens on organisations to develop public versions of their DPIAs. If this recommendation remains, these risks should be acknowledged. Perhaps a better solution than publishing the DPIA might be that organisations might make public in their privacy policies the fact that they have conducted a DPIA as part of their accountability obligations under the GDPR and to ensure that personal data are protected. In addition, it should also be made clear that a decision not to publish a DPIA will not carry negative consequences. For example, not publishing a DPIA should not be an aggravating factor under Article 83(k).

Recommendation: Acknowledge the risks and burdens associated with publishing (parts of) DPIAs and clarify that a decision not to publish a DPIA (or any risk assessment) will not carry any direct or indirect consequences from the DPAs. In addition, it should be confirmed that data subjects cannot ask for access to DPIAs due to the confidentiality of the information. A better alternative than publishing the DPIA might be to include in the organisation's privacy policy a statement that a DPIA was conducted.

8. When shall the supervisory authority be consulted? When residual risks are high.

Mitigation of the risks. The notion of risk mitigation is not sufficiently developed by the WP Guidelines. It should be clearly specified that mitigation does not equal complete elimination of the risk, but rather reduction to the greatest reasonable extent. Risk is inherent in nearly all processing activities; the goal of DPIAs, Privacy by Design and other accountability requirements of the GDPR is to reduce these risks to the extent possible, in balance with the relative benefits to individuals and society.

Moreover, further examples of appropriate measures to reduce the risk should be added, e.g. pseudonymisation, data minimisation and oversight mechanisms. It should be specified that these measures depend on the context.

<u>Recommendation</u>: Clarify in the guidelines the notion of risk mitigation and provide some examples of appropriate measures, as suggested above.

Informal contact with DPAs. Before triggering the official consultation process of Article 36, the WP should specify that a controller can engage in informal contacts with the DPAs.

<u>Recommendation</u>: Specify that a controller can engage in informal contacts with DPAs before engaging in the official consultation of Article 36.

9. Annex I – Examples of existing EU DPIA Frameworks (p. 20)

Relevant methodology and risk standards. The WP cites to two ISO standards—ISO/IEC 2913430 on DPIA methodology (p. 20) and ISO/3100025 on risk management. However, the WP does not mention the *IEEE P7002 Data Privacy Process*.[8] The IEEE project is described as follows:

> The purpose of this standard is to have one overall methodological approach that specifies practices to manage privacy issues within the systems/software engineering life cycle processes. This standard defines requirements for a systems/software engineering process for privacy oriented considerations regarding products, services, and systems utilizing employee, customer or other external user's personal data. It extends across the life cycle from policy through development, quality assurance, and value realization. It includes a use case and data model (including metadata). It applies to organizations and projects that are developing and deploying products, systems, processes, and applications that involve personal information. By providing specific procedures, diagrams, and checklists, users of this standard will be able to perform a conformity assessment on their specific privacy practices. Privacy impact assessments (PIAs) are described as a tool for both identifying where privacy controls and measures are needed and for confirming they are in place.

Although the IEEE project is just getting started, it may also become a relevant resource and should be referred to in the Guidelines.

<u>Recommendation</u>: Consider including it in the Annex. It should also be specified that the industry should be involved in the development of new methodologies.

<u>Conclusion</u>

Thank you for the opportunity to provide further comments on key DPIA and "high risk" questions. We look forward to providing further input in the future as new issues arise, particularly in light of any practical experiences in applying the GDPR DPIA and risk requirements. In the meantime, please do not hesitate to contact us for further information or clarification at bbellamy@hunton.com; mheyder@hunton.com; and hhijmans@hunton.com.

[8] Available at https://standards.ieee.org/develop/project/7002.html.